Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática
Escuela Académico Profesional de Ingeniería de Sistemas

Aplicación del diagrama causa-efecto para identificar los principales riesgos ante un posible siniestro en el planeamiento de una auditoría de procesos

TESINA

Para optar el Título Profesional de Ingeniero de Sistemas

AUTOR

Milagros ARIAS TRUJILLO

ASESOR

José Antonio PÉREZ QUINTANILLA

Lima, Perú

2008

Referencia bibliográfica

Arias, M. (2008). *Aplicación del diagrama causa-efecto para identificar los principales riesgos ante un posible siniestro en el planeamiento de una auditoría de procesos*. Tesina para optar el título profesional de Ingeniero de Sistemas. Escuela Académico Profesional de Ingeniería de Sistemas, Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, Perú.

Dedico la presente tesina a toda mi familia, mis papis, a mis lindas hermanitas Sandra y Angie, pero en especial a mi madre, una gran mujer.

AGRADECIMIENTOS

Al profesor José Pérez Quintanilla, por su orientación y dedicación para que este trabajo cumpla con los objetivos trazados.

A los profesores de la UNMSM, en especial a mis jurados que me apoyaron de manera incondicional con sus sugerencias.

A mis colegas y amigos del trabajo, porque me incentivaron para que culmine este trabajo, es especial a César, un compañero de trabajo que me incentivó en todo momento.

A todas aquellas personas que indirectamente me ayudaron para culminar este trabajo y que muchas veces constituyen un invalorable apoyo.

Y por encima de todo doy gracias a Dios.

Aplicación del Diagrama Causa-Efecto para identificar los principales Riesgos ante un posible Siniestro en el planeamiento de una Auditoría de Procesos

RESUMEN

En la presente tesina mostramos cómo el diagrama Causa efecto puede resultar eficiente al momento de identificar los riesgos críticos de un proceso durante la etapa de planeamiento de una auditoría de Procesos, para que así el programa de auditoría se pueda focalizar en aquellos riesgos que se considerarían los más críticos.

Tenemos que existen muchos marcos de referencia , normas, modelos y metodologías para el análisis e identificación de riesgos, así como también existen diversas herramientas que nos facilitan tales tareas.

El uso de tales herramientas para la identificación de riesgos depende de la realidad de cada organización, utilizando muchas veces más de una herramienta.

Los temas presentados en la tesina se alinean a los nuevos enfoques de procesos y riesgos, que hoy en día están tomando muchas organizaciones, como consecuencia de la globalización, que exige que las empresas sean más eficientes.

Palabras Claves: “Auditoría”, “Procesos”, “Riesgos”, “Diagrama Causa.Efecto”

Application of cause-effect diagram to identify the main risks before a possible Siniestro in the planning of an Audit Process

ABSTRACT

In this dissertation Cause diagram showing how the effect can be efficient at the time of identifying the risks of a critical process during the planning stage of an audit of processes, so that the audit programme can focus on those risks that would be considered the most critical.

We have that there are many frames of reference, rules, models and methodologies for analysis and identification of risks, and there are also various tools that we provide such tasks.

The use of such tools for identifying risks depends on the reality of each organization, using many times more than a tool.

The issues presented in the dissertation are aligned to new approaches and processes risks, which are currently taking many organizations, as a result of globalization, which requires companies to become more efficient.

Key words: "Audit", "Processes", "Risks.", “diagram cause- effect”

ÍNDICE

Capítulo III: Estado Del Arte

Capítulo IV: Caso Práctico

Capítulo V: Conclusiones y Trabajos Futuros

Glosario

Referencias Bibliográficas

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I

INTRODUCCIÓN

1.1 ANTECEDENTES

Al revisar la historia encontramos que la auditoría interna desde la antigüedad ha tenido tres grandes etapas: *La era de la inspección y fiscalización del trabajo* realizado por otros, la segunda época fue la del *enfoque del control interno* y desde la publicación del reporte COSO en los años noventa entramos en la *era de la evaluación del riesgos*. [1]

Los escándalos financieros vinculados a debilidades del control interno orientó a las entidades a utilizar la gestión de procesos y riesgos como herramientas indispensables para el logro de los objetivos estratégicos. Actualmente no se concibe un buen gobierno corporativo sin la incorporación del tratamiento al riesgo y la gestión de proceso en su accionar, lo que obliga a que el enfoque del auditor interno tenga que adoptar la misma dirección.[2]

En 1992, ante la preocupación por mejorar la estructura del control interno tras sucesivos escándalos financieros en los Estados Unidos, surgió el nuevo concepto de control interno COSO, que actualizó su significado e incorporó la evaluación de riesgos como uno de sus cinco principales componentes para lograr una sólida estructura de control interno en la entidad. [2]

[1] Auditoría: Un enfoque Práctico- Autor Benjamín Rolando Téllez Trejo
[2] Los nuevos conceptos del control interno: Informe Coso- Autor Lybrand Cooper

A inicios de la década del 2000, pese a persistentes fraudes con grave repercusión internacional [Caso firma Arthur Andersen - Enron (2000)][3], el concepto de gestión de riesgos comenzó a tomar más fuerza en el ámbito regulatorio y empresarial, difundiéndose el uso de modelos globales como el Estándar Australiano de Administración de Riesgos 43:60, Basilea II, Ley Sarbanes - Oxley, Enterprise Risk Management, y el 2004 con el conocido COSO-ERM.

Sin embargo, antes de dichos sucesos, la auditoría interna venía experimentando deficiencias puntuales. Como ejemplo de este diagnóstico se puede mencionar lo señalado en el "Marco para la evaluación de los sistemas de control interno" publicado por Basilea en enero de 1998.

"En el actual contexto socio-económico globalizado es cada vez más fundamental que las organizaciones sean empresas, administraciones públicas, asociaciones emprendedoras, organizaciones no-gubernamentales puedan ejecutar procesos directivos que respondan al cambio e incertidumbre de los escenarios, a la creciente exigencia de transparencia y conocimiento de la opinión pública y de las partes interesadas, a los principios de sostenibilidad y responsabilidad social; procesos que, después de todo, buscan garantizar la existencia y el éxito de las propias organizaciones. El conjunto de las técnicas y de las metodologías dirigidas a lo que podría definir como "gestión de los procesos de la empresa" es sin duda tan complejo como articulado, también al nivel normativo, debido también a la conocida transversalidad que afecta a menudo a los dominios de conocimiento implicados en aquélla. En cualquier caso, nunca como hoy se percibe la exigencia de una mayor responsabilidad sobre los riesgos que afectan a las diversas actividades humanas.
Se va consolidando una auténtica 'cultura del riesgo' basada, a su vez, en una metodología sistemática y formalizada, la llamada 'gestión del riesgo'

[3] La firma Arthur Andersen auditaba los estados financieros de Enron Corporation, empresa que se declaró en banca rota en medio de un escándalo, perjudicando a sus inversionistas y al Gobierno de EEUU.

capaz de caracterizar el contexto, de estimar –o sea analizar y evaluar- tratar, monitorizar y comunicar los riesgos.[4]

1.2 DEFINICIÓN DEL PROBLEMA

Ante los constantes cambios del ambiente empresarial, la auditoría debe ser sinónimo de asesoría integral.

Aunque comúnmente se piensa que la labor de auditoría es una actividad exclusiva para contadores, lo cierto es que la globalización de la economía sumada a los avances de la tecnología y las comunicaciones han generado nuevos entornos socioculturales que obligan a los auditores a ir más allá de la parte fiscal y financiera, conformando equipos multidisciplinarios que incluyan ingeniero de sistemas, economistas, administradores de empresas, sicólogos, etc. que estén relacionados con la actividad del negocio auditado.[5]

Como consecuencia de la globalización, a las compañías se les exige ser más eficientes, y para lograrlo están tomando la definición de procesos como una buena alternativa, por tal motivo cada día tenemos mas información de los mismos, como por ejemplo la ISO/TC 176/SC 2/N 544R2 , y es por ello, que en la presente tesina presentamos a la Auditoría de Procesos y dentro de la etapa de planeamiento de la misma, identificamos y analizamos los riesgos críticos de un determinado proceso.

En una auditoría de procesos, los auditores enfocan su verificación en un determinado número de actividades existiendo la posibilidad de que dejen de considerar actividades críticas, por tal motivo en la presente tesina, estudiamos la teoría de riesgos, que nos permite identificarlos y así tomar mas atención a aquellas actividades que puedan perjudicar con un mayor impacto a la organización. Para lograr dicho objetivo, utilizamos la técnica

[4] Borghesi A. (Università degli Studi di Verona, Presidente del Comité Científico de ARIMAS, Academic Risk Management Association); Cibien, M. (UNI) Gestión del riesgo y normalización a la búsqueda de un punto de encuentro, 4/10/2005)
[5] Control Interno y Fraudes – Autor: Rodrigo Estupinan Gaitan

del diagrama de causa-efecto, que resulta ser muy útil cuando se deben de identificar y analizar los riesgos más críticos de un determinado proceso.

1.3 OBJETIVO

La presente Tesina, tiene como Objetivo Principal, presentar la técnica del Diagrama de Causa-Efecto como una alternativa al momento de identificar y analizar los riesgos durante la etapa de planeamiento en una Auditoría de Procesos. Asimismo, mostramos los modelos y metodologías para una administración de riesgos.

Para alcanzar este objetivo principal, se tiene **3 objetivos específicos** necesarios.

- ***La adecuada comprensión de los procesos del negocio por los auditores***, facilita un mayor alcance en los procesos auditados, por ello en el presente documento definiremos los temas mas importantes que servirán como base para la identificación de procesos.

- ***Los modelos y las metodologías para la Gestión de Riesgos,*** Describiremos algunos de los modelos y metodologías para la Administración de riesgos.

- Asimismo ***plantearemos la aplicación del diagrama de causa –efecto técnica que ayuda a identificar y analizar los riesgos*** en los procesos del negocio.

1.4 JUSTIFICACIÓN

El análisis de riesgos identificados en un proceso, dentro de la etapa de planeamiento de una Auditoría de Procesos, se alinea al comportamiento evolutivo de los negocios en el mundo, llegando a tener como objetivo principal el de apoyar a los miembros de la empresa en el desempeño de sus actividades, principalmente para que la Alta Dirección adopte decisiones

basadas en las recomendaciones de los informes de auditoría, las mismas que tienen por finalidad advertir hechos relevantes, que puedan traer consigo numerosas pérdidas monetarias, que podrían ser mas eficientes si las auditorías comienzan a centrar su atención en los riesgos más críticos del negocio, por tal motivo se hace necesaria la aplicación de técnicas que faciliten tal hecho, por ello presentamos el Diagrama de Causa-Efecto como un herramienta para la identificación y análisis de riesgos.

1.5 PROPUESTA

En la presente tesina, exponemos los modelos, metodologías y herramientas para realizar el análisis de riesgos de un determinado proceso.
Utilizando el diagrama Causa-Efecto logramos identificar y evaluar los riesgos críticos y/o de mayor impacto que podrían vulnerar a la Organización; dejando de lado aquellos que por su naturaleza no son relevantes y/o trascendentes, con lo cual se estima mejorar la calidad de una auditoria de procesos, dado que el producto final que es el informe constituirá una herramienta mas eficiente para la toma de decisiones por parte de los Directivos.

Para asimilar esta corriente mundial de gestión de procesos y riesgos en el trabajo de auditoría, resulta indispensable efectuar revisiones basada en riesgos y enfocada a procesos críticos y de alto impacto en la organización.

1.6 ESTRUCTURA DE LA TESINA

La presente tesina está organizada en 5 capítulos:

En el capítulo 2 definimos los conceptos necesarios para el mayor entendimiento del tema a tratar, por ejemplo definimos las clases de Auditoría existente, asimismo presentamos el concepto, beneficios de la adecuada gestión de los procesos y los riesgos.

En el capítulo 3 presentamos algunos modelos que sirven de referencia para la gestión de riesgos, entre ellos tenemos a, CobiT, NTP ISO/IEC 17799 de seguridad de Información, Estándar Australiano/Neozelandés, así como también presentamos algunas metodologías que nos indican la forma para realizar tal administración como MAGERIT, y lo propuesto por el PMBOK del PMI, asimismo con la finalidad de presentar un mayor detalle de nuestra propuesta presentamos algunas de las herramientas que se pueden utilizar o adaptar para la identificación y análisis de riesgos como el Diagrama de Afinidad , el Diagrama de Campo de Fuerzas, del diagrama de Causa-Efecto y Lluvia de Ideas .

En el capítulo 4 se detalla el caso práctico, donde se define un proceso y se realiza la auditoría respectiva bajo el enfoque presentado en la tesina.

CAPÍTULO II MARCO TEÓRICO

2.1 QUE ES UNA AUDITORÍA

La palabra auditoría se ha empleado con frecuencia de manera incorrecta y se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas; por eso se ha llegado a acuñar la frase "tiene auditoría" como sinónimo que desde antes de realizarse, ya se encontraron fallas y por lo tanto se está haciendo la auditoría. El concepto de auditoría es más amplio, no solo detecta errores, sino que es un examen crítico que se realiza con el objeto de evaluar la eficiencia y eficacia en una organización.[6]

La palabra auditoría viene del latín auditorius, y de ésta proviene auditor, que tiene la virtud de oír, y el diccionario lo define como "revisor de cuentas auditor". El auditor tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo específico que es el de evaluar la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de recursos alternativos de acción, se tome decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.[6]

La NAGA Normas de Auditoria Generalmente Aceptadas indica lo siguiente.[7] "Los auditores deben seleccionar y aplicar las pruebas y demás procedimientos de auditoria que, según su criterio profesional, sean apropiadas en las circunstancias para cumplir los objetivos de cada auditoria. Esas pruebas y procedimientos deben planearse de tal modo que permitan obtener evidencia suficiente, competente y relevante para

[6] ***Auditoría: Un enfoque Práctico***- Autor Benjamín Rolando Téllez Trejo
[7] ***Normas de Auditoría Generalmente Aceptados***; son los principios fundamentales de auditoría a los que deben enmarcarse su desempeño los auditores durante el proceso de la auditoria.

fundamentar razonablemente las opiniones y conclusiones que se formulen en relación con los objetivos de la auditoria."

La NAGU - Normas de Auditoria Gubernamental aprobado por la Contraloría General de la República del Perú. "La auditoría gubernamental es el examen objetivo, sistemático y profesional de las operaciones financieras y/o administrativas, efectuado con posterioridad a su ejecución, en las entidades sujetas al Sistema Nacional de Control, elaborando el correspondiente informe." [8]

TAREAS PRINCIPALES DE LA AUDITORIA

- Estudiar y actualizar permanentemente las áreas susceptibles de revisión.
- Apegarse a las tareas que desempeñen las normas, políticas, procedimientos y técnicas de auditoría establecidas por organismos generalmente aceptados a nivel nacional e internacional.
- Evaluación y verificación de las áreas requeridas por la alta dirección o responsables directos de la empresa.
- Elaboración del informe de auditoría (debilidades y recomendaciones).
- Otras recomendaciones para el desempeño eficiente de la auditoría.

2.2 TIPOS DE AUDITORÍA

En el presente acápite se establecen las formas de clasificar la Auditoría de acuerdo al modo de ejercer la misma y de acuerdo al área objeto del examen.

En cuanto al modo de ejercer la auditoría se establece la clasificación de la Auditoría en Externa e Interna.

[8] ***Normas de Auditoría Gubernamental*** – NAGU, aprobadas por Resolución de Contaraloría Nº 162-95-CG

En cuanto a la clasificación de acuerdo al área sujeta a examen, se describen las diferentes clases de auditorías de uso común desde este enfoque: Auditoría Gubernamental (Auditoría Financiera, Auditoría de Gestión), Auditoría Integral, Auditoría Informática.

CLASIFICACIÓN POR EL MODO DE EJERCER LA AUDITORIA

Las funciones del Auditor se han extendido hasta exceder el concepto de la auditoría independiente.

Se puede llegar a afirmar que la auditoría es una sola y que esta puede clasificarse teniendo como referencia la manera de ejercerla y el área o sistema de información sujeta a examen.

Si tenemos en cuenta la manera como se ejerce la Auditoría, esta puede clasificarse en Externa e Interna.

2.2.1 AUDITORÍA EXTERNA

Aplicando el concepto general, se puede decir que la auditoría externa o independiente es el examen crítico, sistemático y detallado de un sistema de información de una unidad económica, realizado por un Auditor sin vínculos laborales con la misma, utilizando técnicas determinadas y con el objeto de emitir una opinión in dependiente sobre la forma como opera el sistema, el control interno del mismo y formular sugerencias para su mejoramiento.

Según la Resolución SBS N° 1042-99, en su artículo N°4 indica lo siguiente "La empresa auditora no deberá tener vinculación por propiedad directa o indirecta, de gestión o de parentesco con la empresa o con las personas jurídicas integrantes del conglomerado al cual la empresa pertenece, ni con sus accionistas o socios, directores, gerentes, representantes legales o funcionarios principales, respectivamente, de acuerdo a la normatividad emitida por esta

Superintendencia". El dictamen u opinión independiente tiene trascendencia a los terceros, pues da plena validez a la información generada por el sistema ya que se produce bajo la figura de la Fe Pública, que obliga a los mismos a tener plena credibilidad en la información examinada.[9]

2.2.2 AUDITORÍA INTERNA

"Es el examen crítico y sistemático de los sistemas de control de una unidad económica, realizado por un profesional con vínculos laborales con la misma, utilizando técnicas determinadas y con el objeto de emitir informes y formular sugerencias para el mejoramiento de los mismos. Estos informes son de circulación interna y no tienen trascendencia a los terceros pues no se producen bajo la figura de la Fe Publica."[9]

Las auditorías internas son hechas por personal de la empresa. Un auditor interno tiene a su cargo la evaluación permanente del control de las transacciones y operaciones y se preocupa en sugerir el mejoramiento de los métodos y procedimientos de control interno que redunden en una operación más eficiente y eficaz. Cuando la auditoría está dirigida por auditores independientes, la opinión de un experto desinteresado e imparcial constituye una ventaja definida para la empresa y una garantía de protección para los intereses de los accionistas, los acreedores y el público. Por esto se puede afirmar que el auditor no solamente debe ser independiente, sino parecerlo para así obtener la confianza del público, tal como lo dice la Resolución SBS N° 1041-99, en su artículo 4: "***La Unidad de Auditoría Interna deberá tener la independencia suficiente para cumplir sus funciones de manera efectiva, eficiente y oportuna, contando para ello con todas las facultades para el logro de sus***

[9] NAGU, Normas de Auditoría Gubernamental.

objetivos. Sus integrantes deben estar efectivamente separados de las funciones operativas y administrativas de la empresa."

- DIFERENCIAS ENTRE AUDITORÍA INTERNA Y EXTERNA

Existen diferencias substanciales entre la Auditoría Interna y la Auditoría Externa, algunas de las cuales se pueden detallar así:

	Auditor Interno	**Auditor Externo**
Vínculo entre el auditor y la empresa.	- Vínculo Laboral	- Relación de tipo civil
Habilitada para dar Fe Pública.	- Inhabilitada, debido a la vinculación contractual laboral	-Habilitada legalmente
La evaluación del control interno.	- La evaluación es permanente.	- La evaluación es de forma recurrente.
Independencia	- Limitada frente a terceros por su vínculo laboral	- Absoluta
El examen frente a los hechos.	- Es ipso facto, en el momento.	- Es post facto, después de sucedido los hechos.

Tabla N° 2.1: Auditor Interno Vs. Auditor Externo

CLASIFICACIÓN POR EL ÁREA OBJETO DEL EXAMEN

De acuerdo al área o sistema de información objeto del examen de auditoría, esta se puede clasificar tomando el nombre del área específica o sistema de información examinado. Es así como se tienen Auditoría Financiera, Auditoría de Gestión, Auditoría Operacional, Auditoría Informática, Auditoría Gubernamental, entre las más conocidas. Pero teniendo en cuenta el desarrollo y evolución de la Auditoría, se puede hablar de otras clases, tales como Auditoría Social, Auditoría Ambiental, Auditoría de Mercadeo, Auditoría Médica, etc.

2.2.3 AUDITORÍA GUBERNAMENTAL

La auditoría gubernamental es el examen objetivo, sistemático y profesional de las operaciones financieras y/o administrativas, efectuado con posterioridad a su ejecución, en las entidades sujetas al Sistema Nacional de Control, elaborando el correspondiente informe.

Se debe efectuar de acuerdo a las Normas de Auditoría Gubernamental y disposiciones especializadas emitidas por la Contraloría General de la República del Perú, aplicando las técnicas, métodos y procedimientos establecidos.[10]

Dentro de los objetivos de la Auditoría Gubernamental tenemos los siguientes:

- Evaluar la correcta utilización de los recursos públicos, verificando el cumplimiento de las disposiciones legales y reglamentarias
- Determinar la razonabilidad de la información financiera.
- Determinar el grado en que se han alcanzado los objetivos previstos y los resultados obtenidos en relación a los recursos asignados y al cumplimiento de los planes y programas aprobados de la entidad examinada.
- Recomendar medidas para promover mejoras en la gestión pública.
- Fortalecer el sistema de control interno de la entidad auditada.

Corresponde ejercer la Auditoría Gubernamental a los auditores de la Contraloría General de la República, de los Órganos de Auditoría Interna -OAI de las entidades sujetas al Sistema Nacional de Control y de las Sociedades de Auditoría designadas.

El auditor gubernamental es el profesional que reúne los requisitos necesarios para el ejercicio del trabajo de auditoría en las entidades sujetas al Sistema Nacional de Control, aplicando las Normas de Auditoría Generalmente Aceptadas -NAGA, las Normas Internacionales de Auditoría -NIA y las Normas de Auditoría Gubernamental -NAGU. [10]

Tipos de auditoría gubernamental

La auditoría gubernamental, cuyo tipo se define por sus objetivos, se clasifica en auditoría financiera y auditoría de gestión.

a. Auditoría financiera

"Es aquella que emite un dictamen u opinión profesional en relación con los estados financieros de una unidad económica en una fecha determinada y sobre el resultado de las operaciones y los cambios en la posición financiera cubiertos por el examen la condición indispensable que esta opinión sea expresada por un Auditor debidamente autorizado para tal fin"[11].

El proceso que consiste en el examen crítico, sistemático y representativo del sistema de información financiera de una empresa, realizado con independencia y utilizando técnicas determinadas, con el propósito de emitir una opinión profesional sobre la razonabilidad de los estados financieros de la unidad económica en una fecha determinada y sobre el resultado de las operaciones, cambios en el patrimonio, flujos de efectivo y los cambios en la posición financiera, que permitan la adecuada toma de decisiones y brindar recomendaciones que mejoren el sistema.

[10] Manual de Auditoría Gubernamental - MAGU
[11] ***Auditoría Financiera***, Autor: Jesús Urías Valiente

Objetivos de la Auditoría Financiera: El objetivo principal es opinar si los estados financieros de una empresa presentan, o no razonablemente la situación financiera, el resultado de sus operaciones, y los cambios de su posición financiera.

Según la NAGU, encontramos que el objetivo de la Auditoría Financiera es:

"La auditoría de estados financieros tiene por objetivo determinar si los estados financieros del ente auditado presentan razonablemente su situación financiera, los resultados de sus operaciones y sus flujos de efectivo de acuerdo con principios de contabilidad generalmente aceptados."

b. Auditoría de gestión

La Auditoría de Gestión aunque no tan desarrollada como la Financiera, es si se quiere de igual o mayor importancia que esta última, pues sus efectos tienen consecuencias que mejoran en forma apreciable el desempeño de la organización. La denominación auditoría de gestión se basa en dos clasificaciones que tradicionalmente se tenían: auditoría administrativa y auditoría operacional.

Para entender el concepto de auditoría de gestión es necesario conocer los conceptos tradicionales de auditoría administrativa y auditoría operacional que fueron reemplazados por este último.

Wiilliam P. Leonard presenta la siguiente definición de Auditoría administrativa:
La Auditoría administrativa puede definirse como el examen comprensivo y constructivo de la estructura organizativa de una

empresa de una institución o departamento gubernamental; o de cualquier otra entidad y de sus métodos de control, medios de operación y empleo que dé a sus recursos humanos y materiales.

Joaquín Rodríguez Valencia plantea una definición de Auditoría Operacional así:

Se define como una técnica para evaluar sistemáticamente la efectividad de una función o una unidad con referencia a normas de la empresa, utilizando personal especializado en el área de estudio, con el objeto de asegurar a la administración que sus objetivos se cumplan, y determinar qué condiciones pueden mejorarse.

Los dos anteriores conceptos se han venido manejando de manera tal que se hacía una diferenciación entre auditoría administrativa y auditoría operacional, cuando en la realidad eran dos nombres para un mismo proceso, pues en la práctica no existían diferencias notables entre una y otra.

Sin embargo siguiendo el mismo método para realizar los conceptos de Auditoría es posible afirmar que auditoría de gestión es:

El proceso que consiste en el examen crítico, sistemático y detallado del sistema de información de gestión de un ente, realizado con independencia y utilizando técnicas específicas, con el propósito de emitir un informe profesional sobre la eficacia eficiencia y economicidad en el manejo de los recursos, para la toma de decisiones que permitan la mejora de la productividad del mismo.

La ventaja de ver a la empresa como una totalidad permite al auditor ofrecer sugerencias constructivas, y recomendaciones a un cliente para mejorar la productividad global de la compañía. Es así como la implantación con éxito de la auditoría de gestión puede representar un aporte valioso a las relaciones del cliente.[12]

[12] Sistemas de información para la dirección, Autor: Manfredo Monforte Moreno

2.2.4 AUDITORÍA INTEGRAL

La auditoría Integral evalúa toda la gestión de un ente, midiendo la eficiencia en todos sus aspectos y en todos sus niveles (incluso en la Dirección Superior), no solo establece los defectos sino que propone mejoras. Por lo general la realiza un consultor auditor externo, puede llegar a realizarla un auditor interno, siempre y cuando actúe como staff en función delegada por la Dirección Superior y aplique los criterios de la auditoría integral. [13]

2.2.5 AUDITORÍA DE PROCESOS

Con la publicación de las revisiones de la familia de normas ISO 9000, existe más interés en el enfoque sobre el proceso para manejar una organización. El principio N° 4 de la gestión de calidad establece que "un resultado deseado se logra de manera más eficiente cuando las actividades y los recursos necesarios son administrados como parte de un proceso." El aumento de la atención a los procesos naturalmente conlleva al incremento en la atención a las auditorías de procesos. Aún así, muchos tratan a las auditorías de proceso como si fuera un pequeño sistema de auditoría. Auditar los procesos no es lo mismo que un proceso de auditoría. En ambas formas de auditoría existen similitudes, pero también existen diferencias fundamentales. [14]

Las auditorías de procesos son sistemas abiertos, en contraposición a las auditorías de procedimientos que básicamente se realizan bajo un entorno cerrado cuyo núcleo es la empresa y/u organizaciones departamentales. Cuando se realiza una auditoría de sistemas por procedimientos, los equipos auditores preparan cuestionarios como

[13] Manual de Auditoría Integral y Ambiental Editorial Osmar Buyatti –Argentina 1998
[14] Auditorías de calidad para mejorar la productividad – Autor: Dennis R. Arter

herramienta auxiliar para el trabajo de campo; ahora en el enfoque a procesos no es fácil disponer de listas cerradas dado que el motor director de la auditoría será el proceso y a priori éste no es conocido. Sin duda, será necesario crear cuestionarios específicos por procesos, sean éstos estratégicos, operativos, de soporte o de medida en el momento de revisar la documentación aplicable al alcance y objetivo de la auditoría. [15]

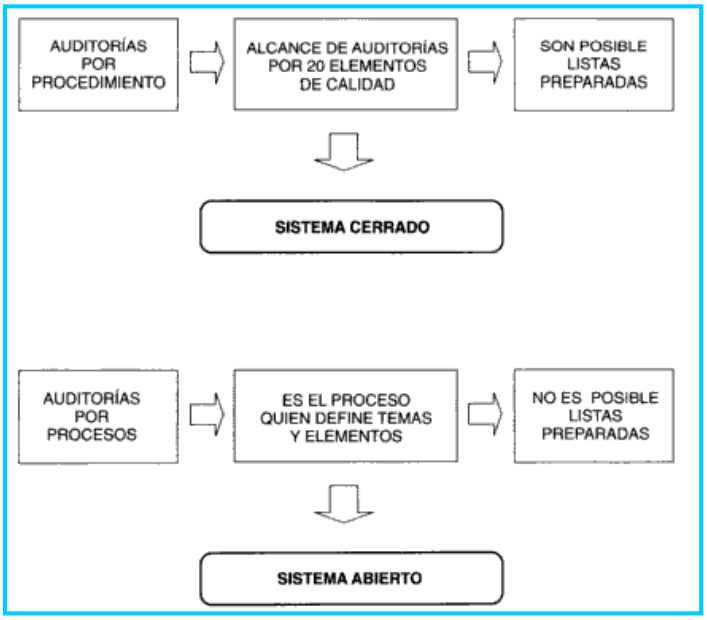


Figura 2.1 : Auditoria de Procesos

Asimismo, la auditoría de procesos permite una evaluación horizontal y vertical, cruzando las barreras entre diferentes unidades funcionales y unificando sus enfoques hacia los beneficios principales de la organización.

[15] La transición a las nuevas ISO 9000:2000 y su implantación – Autor: Joseph Cervera

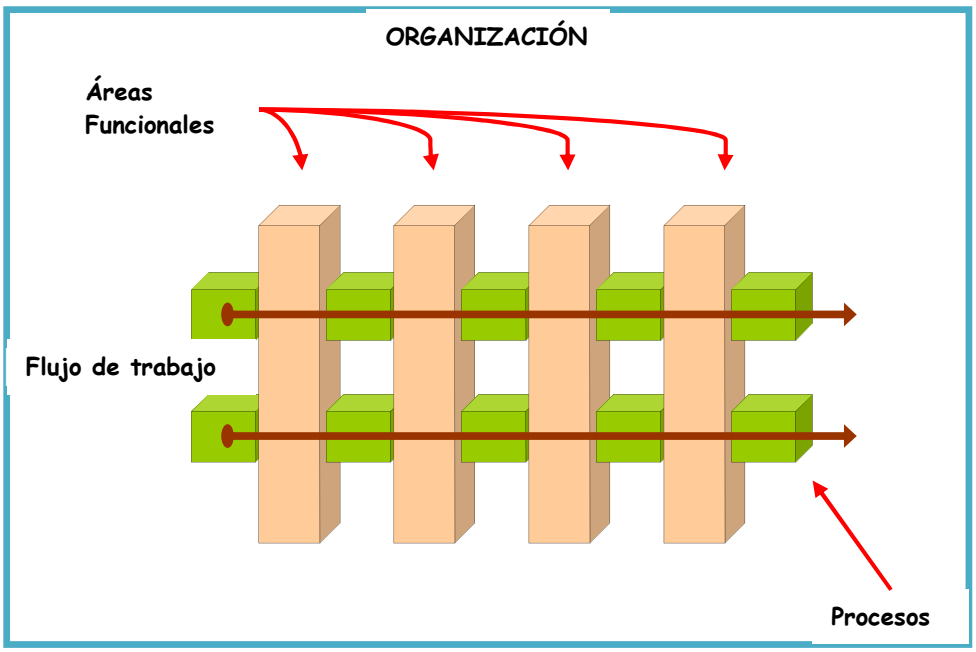


Figura N° 2.2: Áreas Funcionales Vs. Procesos

2.2.6 AUDITORÍA INFORMÁTICA

La auditoría Informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantienen la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. Des este modo la auditoría informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoría:

- Objetivos de protección de activos e integridad de datos.
- Objetivo de gestión que abarcan, no solamente los de protección de activos, sino también los de eficacia y eficiencia.

El auditor es responsable de revisar e informar a la Dirección de la Organización sobre el diseño y el funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada.
Se pueden definir 3 grupos de funciones a realizar por un auditor informático:

- Participar en las revisiones durante y después del diseño, realización implantación y explotación de aplicaciones informativas.
- Revisar y juzgar los controles implantados en los sistemas de información para verificar si están adecuados a las instrucciones de la Dirección, requisitos legales, cobertura de errores, fraudes.
- Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información.[16]

2.3 CONTROL INTERNO

Definición

El Control Interno es una Multitud de Procesos por lo que está orientado hacia un fin, pero no es un fin en sí mismo, no son manuales de políticas y formularios, es llevado a cabo por personas a todo nivel jerárquico.

El Control Interno provee sólo de certeza razonable, no absoluta, a la gerencia y el Directorio.

Un buen control interno no puede garantizar el éxito de una organización, pero un mal control interno puede garantizar el fracaso de la misma.

El control interno es[17]:
-Un proceso integral, El control interno no es un hecho o circunstancia, sino una serie de acciones que están relacionadas con las actividades de la entidad. Estas acciones se dan en todas las operaciones de la entidad continuamente. Estas acciones son inherentes a la manera en la que la gerencia administra la organización. El control interno por lo tanto es diferente a la perspectiva que tienen algunos de él, quienes lo ven como un hecho adicionado a las actividades de la entidad, o como una obligación.

[16] Auditoría Informática: Un enfoque práctico –Autor: Mario Piattini
[17] Guías para las Normas del Control Interno del Sector Público

-Efectuado por la gerencia y el resto del personal, La gente es la que realiza el trabajo de control interno. Éste se logra por los individuos dentro de una organización, con lo que ellos hacen y dicen. Consecuentemente el control interno es ejecutado por la gente. La gente debe conocer su rol, sus responsabilidades, y los límites de autoridad.

-Dar respuesta a los riesgos, Cualquiera que sea la misión de la entidad, su consecución se enfrentará a toda clase de riesgos. La tarea de la gerencia es identificar y dar respuesta a estos riesgos para maximizar la posibilidad de alcanzar la consecución de la misión. El control interno puede ayudar a enfrentarse a estos riesgos, sin embargo sólo puede proporcionar una garantía razonable sobre el logro de la misión y de los objetivos generales.

-Provee seguridad razonable*,* No importa cuan bien diseñado y ejecutado esté, el control interno no puede dar a la gerencia seguridad completa en relación al logro de los objetivos generales. En su lugar, las directrices dicen que se puede esperar un nivel "razonable" de seguridad. La seguridad razonable equivale a un nivel satisfactorio de confianza bajo ciertas consideraciones dadas de costo, beneficio y riesgo, y equivale a un nivel satisfactorio de confianza bajo ciertas consideraciones dadas de costo, beneficio y riesgo.

Logro de objetivos, El control interno está dirigido hacia el logro de una serie de objetivos generales, objetivos separados pero al mismo tiempo integrados. Estos objetivos generales son los siguientes:

- Ejecución ordenada, ética, económica, eficiente y efectiva de las operaciones
- Cumplimiento de las obligaciones de responsabilidad
- Cumplimiento de las leyes y regulaciones aplicables
- Salvaguarda de los recursos para evitar pérdidas, mal uso y daño.

Dentro de las limitaciones del control Interno tenemos que no puede por sí mismo asegurar el logro de los objetivos, dado que depende del factor humano, por ello es sujeto a las debilidades en el diseño, errores de juicio o interpretación, mala comprensión, descuido, fatiga, distracción, colusión, abuso o excesos, otro factor limitante es que el diseño del sistema de control interno se enfrente a la disminución de recursos. Los beneficios de los

controles deben ser considerados consecuentemente en relación a su costo. Mantener un sistema de control interno que elimine el riesgo de pérdida no es realista y probablemente costaría más que los beneficios derivados.

Al determinar si un control particular debe o no ser diseñado, la probabilidad de que exista un riesgo y el efecto potencial de éste en la entidad deben ser considerados junto con los costos relacionados a la implantación del nuevo control.

2.4 COMPONENTES DEL CONTROL INTERNO.

El control interno comprende cinco componentes interrelacionados como lo vemos en la siguiente imagen:

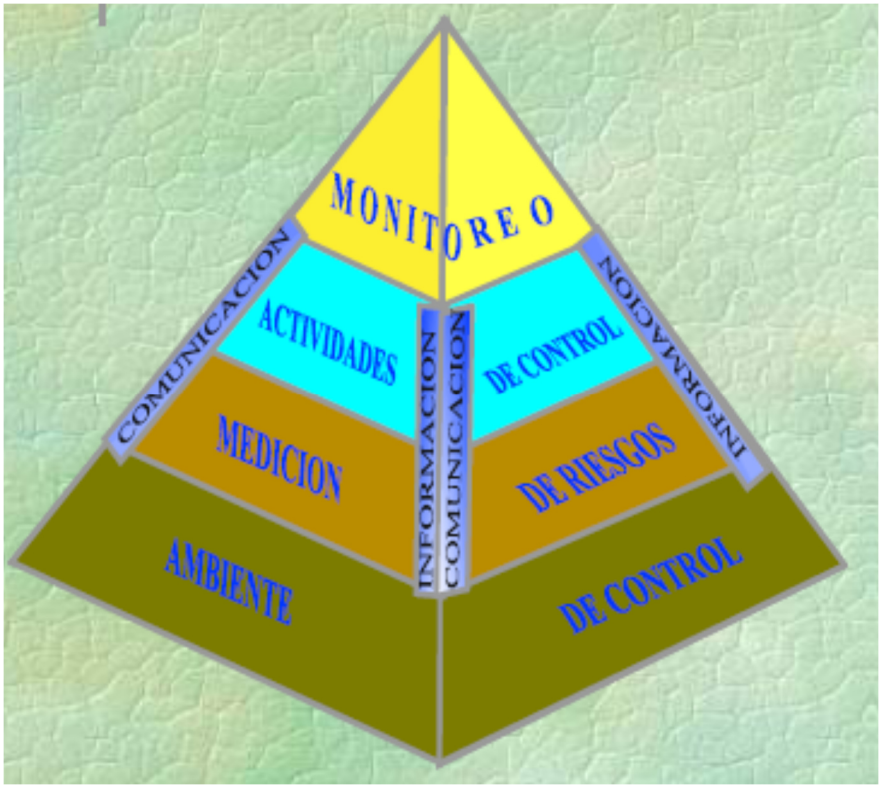


Figura N°2.3: Componentes del Control Interno

Fuente: *Guía para las normas de* control interno del sector público - Fr. VANSTAPEL

2.4.1 AMBIENTE DE CONTROL

Está referido a atributos que incluyen la integridad, valores éticos, habilidades y el ambiente en el que estos se desarrollan. Es el punto central de cualquier empresa y su personal

Representa la forma de ser y operar de una organización, caracterizada por la actitud y compromiso de la alta dirección con el Sistema de Control Interno, así como por las pautas de comportamiento del personal de la organización, para que sus actuaciones sean consecuentes con los valores adoptados en la empresa.

El ambiente de control es expresión de la filosofía de la administración, la cual determina los niveles de autoridad, responsabilidad y organización del talento humano.

Los valores son ante todo realidades que tienen una función central en la vida social.

Es una cualidad de la persona o de las cosas y al poseer esta cualidad se hace deseable o estimable a los demás.

2.4.2 EVALUACIÓN DE RIESGO

Este componente del control interno, es el proceso de identificar y analizar los riesgos relevantes para la consecución de los objetivos de la organización y determinar una respuesta apropiada.

La empresa debe estar consciente de los riesgos. Al mismo tiempo debe establecer mecanismos para identificar, analizar y gerenciar los riesgos relacionados con su operación y entorno.

Es un proceso permanente e interactivo que lleva a que continuamente la administración en coordinación con la oficina de control interno o

quien haga sus veces, revalúe los aspectos, tanto internos como externos que pueden llegar a representar amenazas para la consecución de los objetivos organizacionales.

De igual manera, implica la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación de los riesgos asociados con una determinada actividad o con la organización en general, con el fin de preparar a las organizaciones para minimizar pérdidas y maximizar sus ventajas.

Valoración del Riesgo

Es fundamental establecer la estructura del riesgo en la empresa partiendo con los riesgos del nivel estratégico asociados a factores externos (económicos, sociales, políticos-legales y tecnológicos); asimismo, los riesgos basados en factores internos que entre otros representan los sistemas de información (vulnerabilidad), el personal vinculado (respecto a su calidad y motivación) la naturaleza de los procesos.

Manejo del Riesgo

Este es un punto importante, ya que los esfuerzos en la "Valoración del riesgo" llegan a ser en vano si no se realiza un adecuado manejo y control de los mismos, y dentro de las acciones a tomar pueden ser tales como la implantación de políticas, estándares, procedimientos y cambios físicos entre otros, que hagan parte de un plan de manejo que conlleve a evitar, reducir, dispersar y atomizar el riesgo, o en último caso asumir el riesgo.

Monitoreo

Es necesario monitorear permanentemente el plan de manejo de riesgos, ya que éstos nunca dejan de representar una amenaza para la organización, es decir, no se eliminan, sólo se mitigan.

2.4.3 ACTIVIDADES DE CONTROL.

Las actividades de control son las políticas y procedimientos de control para asegurar que las acciones identificadas por la gerencia como necesarias para manejar el riesgo y alcanzar los objetivos de la empresa están siendo llevadas a cabo eficientemente.

Las actividades de control ocurren a través de la organización, en todos los niveles y en todas las funciones. Las actividades de control hacen parte del proceso mediante el cual la empresa intenta lograr sus objetivos de negocio.

Para que las actividades de control sean efectivas deben de encontrarse dentro de un plan, con un determinado costo y deben estar relacionadas directamente con los objetivos de control.

Las empresas deben alcanzar un equilibrio entre la detección y la prevención de las actividades de control.

Actividades de control de información tecnológica

Los controles de información tecnológica se dividen en dos grandes grupos:

(1) Controles generales
Son la estructura, políticas y procedimientos que se aplica al segmento de la información de la empresa asegurando su correcta operatividad y

de ese modo crear el medio en el que operan los sistemas de aplicación y los controles.

(2) Aplicación de controles

Las políticas y procedimientos se aplican por separado a los sistemas de aplicación individual, y están directamente relacionados a las aplicaciones individuales computarizadas. Estos controles están generalmente diseñados para prevenir, detectar y corregir errores e irregularidades mientras la información fluye a través de los sistemas de información.

2.4.4 INFORMACIÓN Y COMUNICACIÓN

Estos permiten a los empleados capturar e intercambiar la información necesaria para organizar, dirigir y controlar sus operaciones.

Se tiene que identificar, capturar y comunicar información interna y externa de una forma y en un determinado tiempo que le sea permitido al personal de la empresa llevar a cabo sus responsabilidades.

La comunicación no sólo existe dentro de la empresa, sino también con las partes externas, tales como clientes, proveedores, reguladores y accionistas.

Se requiere información en todos los niveles de la organización para identificar, valorar y responder a los riesgos, y de este modo lograr los objetivos de la empresa.

La organización deberá establecer una infraestructura de sistemas de información para obtener, capturar, procesar, analizar y reportar los grandes volúmenes de información, que ayudarán en la toma de decisiones de la empresa. Estos sistemas de información son percibidos en el con texto del proceso de datos generados internamente.

2.4.5 MONITOREO

Todo el proceso debe ser supervisado y las modificaciones deben ser realizadas según se necesiten. De esta manera el sistema puede reaccionar dinámicamente, cambiando según las condiciones lo requieran.

El monitoreo debe asegurar que los hallazgos de auditoría y las recomendaciones sean adecuados y oportunamente resueltos.

El seguimiento se logra a través de actividades rutinarias, evaluaciones puntuales o la combinación de ambas.

(1) *Seguimiento continuo:*
Las actividades del seguimiento continuo cubren a cada uno de los componentes del control interno, asimismo involucran acciones contra los sistemas de control interno irregulares, antiéticos, antieconómicos, ineficientes e ineficaces.

(2) Evaluaciones puntuales:
Éstas evaluaciones dependen de la valoración de los riesgos y de la efectividad de los procedimientos del monitoreo, asegurando que el control interno logre los resultados deseados basándose en procedimientos, también es importante indicar que todas las deficiencias del control interno deben de ser reportadas al nivel adecuado de la gerencia.[18]

- **LIMITACIONES DEL CONTROL INTERNO**

Esto se debe a los factores limitantes como los siguientes:

[18] Guía Metodológica para el Fortalecimiento y Evaluación del Sistema de Control Interno

Fracasos

La gente que tiene la responsabilidad de los controles puede no realizarlos en forma eficiente, no todos están capacitados para tales tareas.

Disfunciones del Sistema

Dejadez, fatiga o despistes, origina que el personal no tome interés en su difusión.

Transgregación Gerencial

Un gerente puede eludir intencionalmente las prácticas establecidas debido a fines inadecuados.

Confabulación

Dos o más personas pueden colaborar para quebrar los controles.

Costo vs. Beneficios

Los recursos son limitados. Los Gerentes aceptan correctamente un grado de riesgo cuando el costo del control de ese riesgo excede el beneficio.

2.5 LOS PROCESOS

Actualmente muchas organizaciones miden sus actividades según el enfoque de procesos, para alcanzar y controlar de manera eficiente la gestión empresarial.

Tenemos que a una organización se le puede considerar como un conjunto de procesos y red de transacciones. Para que dicha organización funcione de forma eficaz es necesario identificar las numerosas actividades que están relacionadas[19] .

[19] La nueva familia de normas internacionales ISO 9000 se basan en ocho principios fundamentales que vienen a representar el marco hacia la mejora del desempeño del Sistema de Gestión de Calidad en una organización. Uno de los ocho principios es el de enfoque por procesos, el cual plantea que un "resultado deseado se alcanza más eficientemente cuando las actividades y los recursos relacionados se gestionan como un proceso".

- **Objetivos de Negocio**

"Estos son esencialmente organizacionales y corresponden a los intereses particulares de un ente económico"[20]

Los procesos de la organización persiguen un objetivo de manera independiente, que al ser integradas dan como resultado el objetivo de la organización o el objetivo de negocio.

Es posible definir el objetivo de negocio de una determinada organización, con la intención de tener un marco de referencia al momento de auditar sus procesos, así como también definir responsabilidades e identificar quienes son las personas a las que les afectaría o beneficiaría de manera directa o indirecta algún evento de un proceso determinado, éstas personas son los llamados Stakeholders (grupos de interés de una determinada organización que tienen intereses directos e indirectos en una determinada empresa).[21]

Tales Stakeholders pueden ser los accionistas de la organización, los clientes, competidores, dueños, personal en general, gobiernos locales, nacionales o internacionales, sindicatos, proveedores, etc, todos estos stakeholders sacan beneficio o sufren daños como resultado de las acciones de la empresa, y por ende se ven afectados ante cualquier eventualidad de los procesos que constituyen la organización.

[20] "Auditoria de Control Interno" Autor: Samuel Alberto Mantilla Blanco
[21] ***Los StakeHolders y la Acción social de la empresa*** – Autor: Autor Juan Luis Martínez, Mariá Carbonell, Ana Agüero, Fundación Rafael del Pino

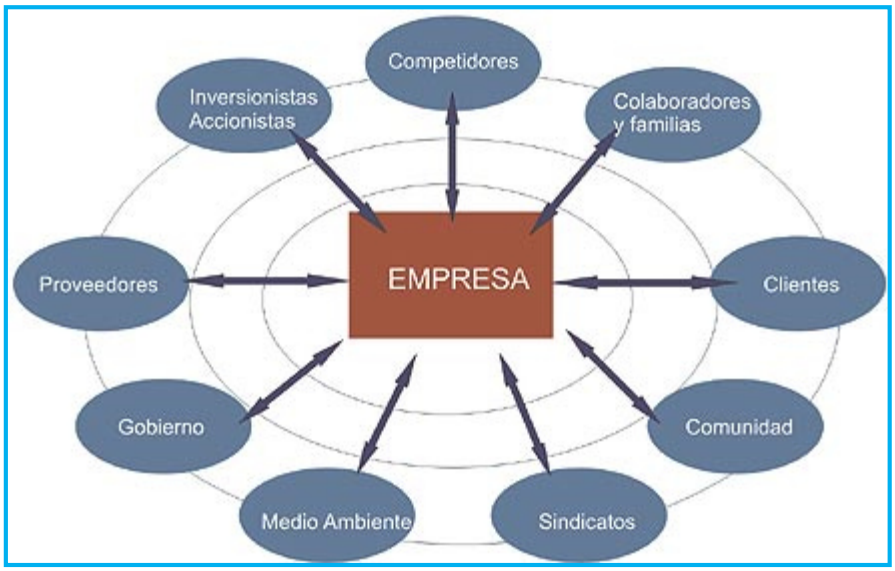


Figura N° 2.4 Stakeholders de una organización

- **Definición de Procesos**

Una actividad que emplea recursos y que los gestiona para facilitar la transformación de sus entradas en resultados, es considerado como un proceso.

El concepto de proceso siempre existió en el pasado, pero evolucionó a través de los cambios industriales. Actualmente no se puede hablar de control de calidad sin haber utilizado para su medición la teoría de procesos, del mismo modo que la reingeniería o mejora continua en la gestión empresarial.

"Un proceso es una serie de actividades que toman un insumo y lo transforman para crear un producto".[22]

[22] Mc Hugh/Wheeler (1993) Reingeniería de procesos de negocios, LIMUSA, México.

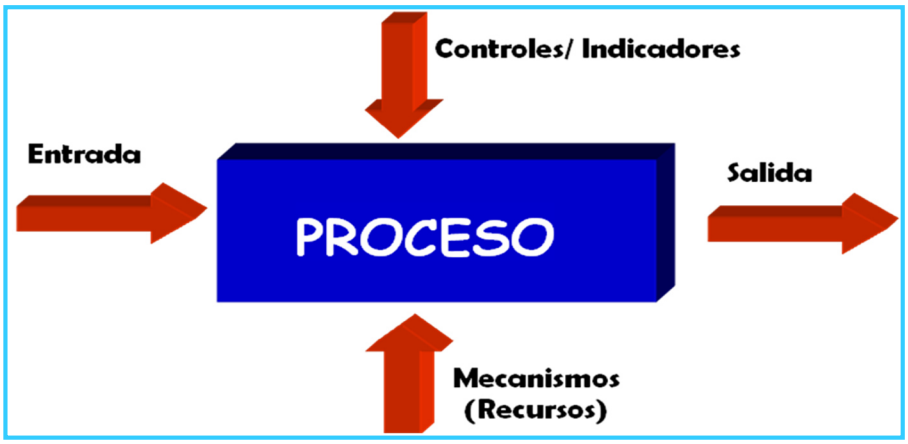


Figura N°2.5: Marco del Proceso

Heras[23] define como proceso "al conjunto de actividades secuenciales que realizan una transformación de una serie de inputs (material, mano de obra, capital, información, etc.) en los outputs deseados (bienes y/o servicios) añadiendo valor".

"No existe producto y/o servicio sin un proceso. De la misma manera, no existe proceso sin un producto o servicio. Proceso es cualquier actividad que emplee un insumo, le agregue valor a éste y suministre un producto a un cliente externo o interno. Los procesos utilizan los recursos de una organización para suministrar resultados definitivos."[24]

Algunos tipos de procesos suelen estar como funciones en una organización jerárquica. Si bien todas las unidades organizacionales cumplen sus funciones a cabalidad, es frecuente experimentar situaciones en la que muchas organizaciones no tengan una visión clara de procesos.

Por otro lado, los procesos pueden ser físicos, incluir papeleo, ser realizados por computadora, o ser una secuencia lógica de eventos.

Desde este punto de vista, una organización estructurada por actividades también puede ser considerada como un sistema de procesos más o menos

[23] Heras, M. (1996) Gestión de la producción, ESADE, Barcelona
[24] H.J. Harrington (1994) Mejoramiento a los procesos de la empresa, McGraw-Hill Interamericana S.A., Colombia.

relacionados entre sí, en la que una buena parte de las entradas generadas interna o externamente tendrán resultados hacia los clientes internos o externos. [25]

Esta orientación muchas veces puede hacer que el ámbito y alcance de los procesos no sea homogéneo, teniendo que ser definido cada caso en forma especial, sobre todo cuando prevalecen factores de tamaño o de cierta complejidad. Esto quiere decir que a veces, cuando no es tan evidente dónde se inicia y dónde finaliza un proceso, es necesario establecer una delimitación por efectos operativos, de dirección y de control del proceso, pudiendo recurrir a la segmentación de subprocesos si fuera el caso. También suele ocurrir que un proceso puede ser realizado por una sola persona dentro de una misma unidad organizacional. Sin embargo, los más complejos fluyen en la organización a través de diferentes áreas funcionales.

El hecho que en un proceso intervengan distintas unidades dificulta su control, diluyendo la responsabilidad que esas unidades tienen sobre el mismo. En resumen, cada área suele responsabilizarse del conjunto de actividades que desarrolla o le fueron asignadas, pero la responsabilidad y compromiso con la totalidad del proceso suele no ser tomado por nadie en concreto.

En la gestión de las empresas un proceso se define como "un conjunto de actividades elementales interrelacionadas entre sí que transforman una entrada en una salida, consumiendo unos recursos y aportando valor."

La gestión por procesos introduce en las clásicas organizaciones verticales una visión y forma de actuar transversal, que adiciona valor a un producto que internamente se transfiere de un departamento a otro y finalmente es ofrecido como servicio al cliente.

[25] ***Guía para una gestión basada en procesos*** – Autor: Jaime Beltrán Sanz

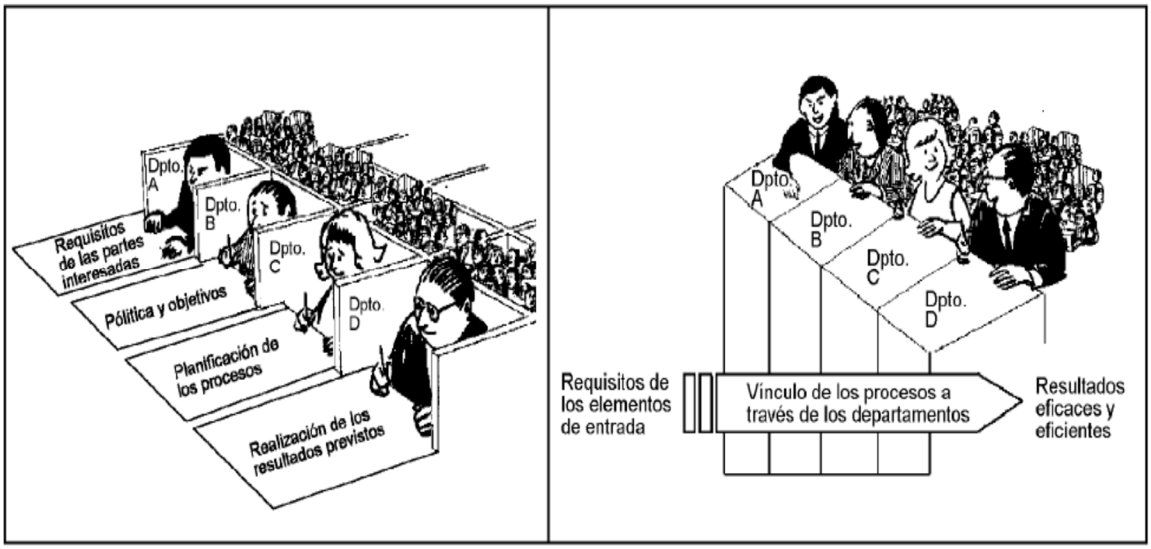


Figura N°2.6: Ejemplo de vínculo de los procesos a través de los departamentos en una organización
Fuente: ISO 2004

Se habla realmente de proceso si cumple las siguientes características o condiciones:

- Se pueden describir las entradas y las salidas.
- El proceso cruza uno o varios límites organizativos funcionales.
- Una de las características significativas de los procesos es que son capaces de cruzar verticalmente y horizontalmente la organización.
- El proceso tiene que ser fácilmente comprendido por cualquier persona de la organización.
- El nombre asignado a cada proceso debe resultar de los conceptos y actividades incluidos en el mismo.

Centrarse en los procesos de la empresa permite lo siguiente:

- Orientarse al cliente
- Permite controlar el cambio
- Aumenta la competitividad
- Previene errores y ayuda a corregirlos
- Evaluación integral

Otros términos relacionados con la determinación de procesos, y que son necesarios tener en cuenta para facilitar su identificación, selección y definición son los siguientes:

Subprocesos: Son partes bien definidas en un proceso. Su identificación puede resultar útil para aislar los problemas que pueden presentarse y posibilitar diferentes tratamientos dentro de un mismo proceso.

Actividad: Es la suma de tareas, normalmente se agrupan en un procedimiento para facilitar su gestión. La secuencia ordenada de actividades da como resultado un subproceso o un proceso. Normalmente se desarrolla en una unidad.

Tarea: Forma específica de llevar a cabo una actividad. En muchos casos se especifican mediante procedimientos expresados en documentos que contienen el objeto y el campo de aplicación de una actividad; qué debe hacerse y quien debe hacerlo; cuando, donde y como se debe llevar a cabo; que materiales, equipos y documentos deben utilizarse; y como debe controlarse y registrarse.

Indicador: Es un dato o conjunto de datos que ayudan a medir objetivamente la evolución de un proceso.

Por la naturaleza del resultado final, los procesos pueden ser de producción, cuando el resultado final es un bien determinado; de servicios, cuando sea un bien intangible; y administrativo, cuando el fin es un acto administrativo, sobre todo como apoyo en la consecución de la producción de un bien o servicio.

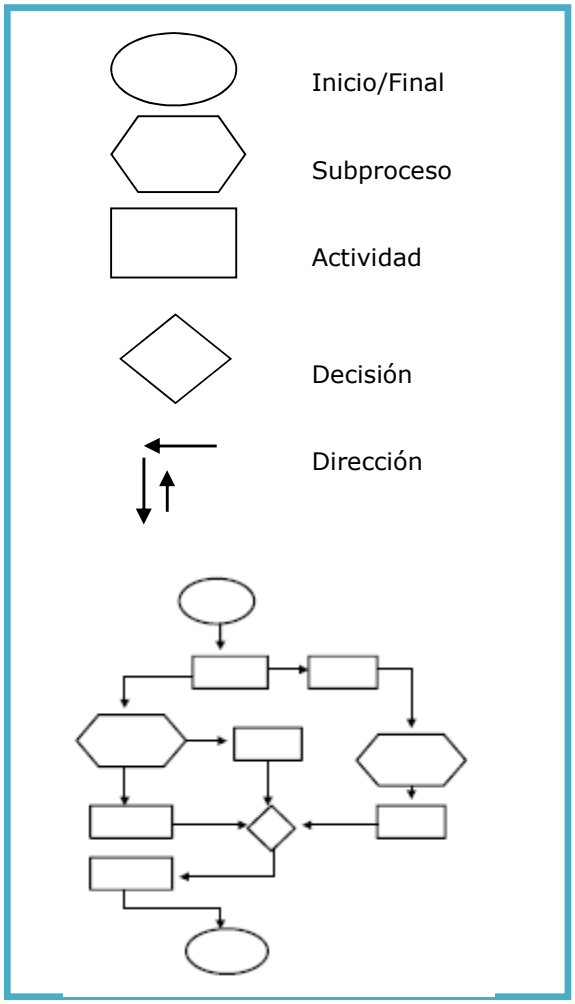


Figura N°2.7: Diagrama de flujo

Durante la producción de bienes se designan como procesos a las tareas manuales, los sistemas de coordinación entre los trabajadores y maquinarias, y también a los procesos automatizados.

En la producción de servicios denominamos procesos a aquellos no relacionados con la producción de bienes, podemos mencionar al proceso de transporte, asistencia de limpieza, entre otros.

Los procesos además tienen que tener indicadores que permitan visualizar de forma gráfica la evolución de los mismos. Tienen que ser planificados, asegurar su cumplimiento, realizar el seguimiento y ajustar y/o establecer objetivos.

El diagrama de flujo es una representación gráfica que muestra todos los pasos de un proceso. Es una excelente herramienta que mediante el empleo de símbolos fáciles permite representar las relaciones involucradas en un proceso.
Mediante el estudio de estos diagramas se pueden descubrir vacíos que pueden ser fuente potenciales de problemas.

Existen muchos métodos para la identificación de procesos, los que se pueden englobar básicamente en dos grandes grupos:[26]

Método Estructurado: Se incluyen aquellos que sirven para su identificación según modelos estandarizados. Estos están diseñados por expertos y su implantación requiere autorización formal u oficial.

Método Creativo: Son aquellos que se idean e implantan de forma interna, normalmente motivadas por lluvia de ideas y de experiencias.

La elección del método dependerá del conocimiento que tengan los miembros de la empresa y/o del "estado del arte" en el cual se encuentre la misma.

Muchas veces es mejor escoger el método estructurado y recurrir a una asesoría, por supuesto tras sopesar los inconvenientes de la misma. También podría ser una combinación de ambas.

2.6 LOS RIESGOS

La oportunidad de que algo ocurra que tendrá un impacto sobre los objetivos. Esta medida en términos de consecuencia y posibilidad.[27]

El paradigma tradicional sobre el riesgo era que:

- El riesgo era malo por naturaleza.

[26] ***Innovación de procesos***, Autor: Thomas H. Daveport
[27] Estándar Australiano/Neozelandés

- Antes como todo era funcional (comercial, financiero, producción, etc), originó que el riesgo sea reconocido como responsabilidad de la función de seguridad en las empresas.
- Existía la creencia de fijar como meta la eliminación del riesgo.
- Se pensaba que la seguridad la definía un experto.
- El control de pérdidas era el lenguaje clave para entender los riesgos.

La percepción general de hoy es que la administración del riesgo es integral[28], necesaria, que se gasta mucho dinero y que se obtienen pocos resultados.

Todas las organizaciones durante la vida de funcionamiento están sometidas en forma permanente a amenazas o causas de riesgos de diversa índole, ya sean de origen natural (p.ej. terremotos), tecnológico (p.ej. pérdida información) o social (p.ej. terrorismo), que pueden afectar sus objetivos.

Para conocer con claridad la teoría de riesgos, primero se debe conocer la diferencia que existe entre siniestro y riesgo.[29]

Siniestro, es un evento o acto producido no deseado con capacidad de generar efectos negativos.
Riesgo, la posibilidad de que suceda algo que tendrá un impacto sobre los objetivos. Se mide en términos de consecuencias y probabilidades.

Los siniestros pueden ser:
- *Accidentales:* Origen fortuito.
- *Voluntarios:* Origen intencional.

Se define también como siniestro a todo evento repentino no planeado, que pueda tener consecuencias negativas (daños, lesiones, pérdidas, etc). Es un suceso incierto cuya ocurrencia da lugar a la materialización del riesgo.

[28] Se ha dejado de considerar el manejo aislado de riesgo financiero, operacional y de tecnología de información por un enfoque integral de riesgos.
[29] Estándar Australiano/Neozelandés

El proceso de generación de un siniestro nace en la existencia de deficiencias de las causas o factores internos del proceso, ya sea que ellos se originen en las acciones u omisiones de personas o en las malas condiciones materiales reinantes. Estos factores pueden desencadenar en un evento con consecuencias sobre personas, bienes o la organización, y todo ello se reflejará en un impacto de pérdida económica. Como vemos, el evento es la ocurrencia de un conjunto de circunstancias. Una sola ocurrencia o varias pueden generar pérdida con una consecuencia negativa financiera o de otro tipo.

La consecuencia es el resultado final de un evento. Puede haber más de una consecuencia en un evento. Las consecuencias pueden ser expresadas cualitativamente o cuantitativamente.

Como vemos, un siniestro es un hecho ocurrido; mientras que el riesgo mide la expectativa de que pueda ocurrir algo que todavía no sucedió.

A la sucesión de actividades que pueden activar un evento se le llama amenaza o causas de riesgos, que ante la frecuencia que se presente tiene la probabilidad de que ocurra un siniestro. La característica básica es que debe haber siempre una exposición de estas amenazas. [30]

Toda amenaza o causa de riesgos tiene que cuantificarse, es decir medir la probabilidad de que ocurra. Podría decirse que amenaza es un riesgo no evaluado en sus consecuencias.

[30] NTP ISO/IEC 17799:2007 – Norma Técnica Peruana

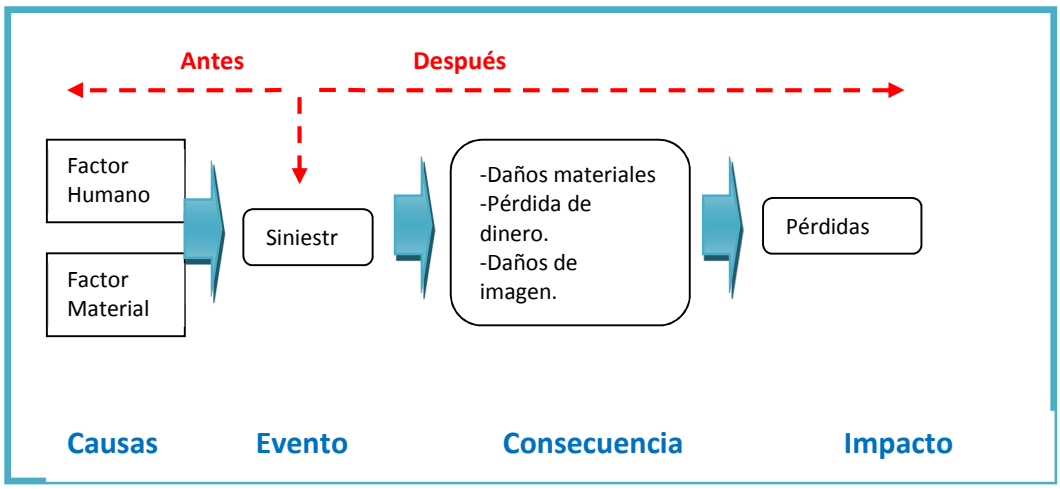


Figura N°2.8: Proceso del Siniestro

Las amenazas o causas de riesgos pueden permanecer latentes sin llegar a afectar al proceso o también eventualmente pueden materializarse en un evento dañino con consecuencias y efectos negativos variados, tal como lesiones o muertes, daños materiales, pérdidas económicas, suspensión de la operación, pérdida de información o daño ambiental.

Por consiguiente, el riesgo es medir como se relaciona la probabilidad de que afecten las amenazas con la generación de probables consecuencias. La probabilidad de que, en ciertas condiciones de exposición, las amenazas o causas de riesgos presentes puedan en un periodo de tiempo materializarse en un siniestro con determinadas consecuencias sobre los elementos expuestos, se denomina comúnmente riesgo.

Existen riesgos puros[31] (operacionales) y riesgos especulativos[32] (negocio). La vinculación de riesgos operacionales más especulativos depende del perfil del negocio. El ideal es que todos los niveles de riesgos sean aceptables, pero es utópico debido a que están expuestos a muchos factores exógenos.

En líneas generales se considera que el riesgo tiene tres componentes básicos: el evento, la probabilidad de que este ocurra y las consecuencias

[31] Es el que se da en la empresa y existe la posibilidad de perder o no perder pero jamás ganar.
[32] Es aquel riesgo en la cual existe la posibilidad de ganar o perder, como por ejemplo las apuestas o los juegos de azar.

asociadas al mismo. En tal sentido las variables vinculadas a los riesgos son:

- Frecuencia (Amenaza o causas de riesgos)
- Consecuencias (Vulnerabilidad)

Es importante advertir la siguiente diferencia:

- Siniestro es el pasado, ya ocurrió.
- Riesgo es futuro, podría ocurrir.

El siniestro se mide por estadísticas, mientras que el riesgo por probabilidades.

Los riesgos se pueden clasificar:

- Por sus consecuencias: riesgos puros y especulativos.
- Por su origen: riesgos naturales, tecnológicos y sociales.
- Por su evolución: riesgos estáticos y dinámicos.
- Por su alcance: riesgos individuales y colectivos.
- Por su intensidad relativa: riesgos insignificantes, marginales, graves, críticos, desastrosos y catastróficos.
- Por su aceptabilidad: riesgos aceptables, tolerables, inaceptables e inadmisibles.

2.6.1 CLASIFICACIÓN DE RIESGO

Existen muchas clasificaciones de los Riesgos, pero es importante que cada organización tenga su propio Perfil de Riesgos, y para ello es necesario conocerlos y diferenciarlos.

Aquí tenemos la Clasificación de Riesgos según "El Modelo de Riesgos de Negocios de Protiviti" que podría ser considerado como base a la hora de definir un Perfil de Riesgos:[33]

I. RIESGOS DEL ENTORNO

El riesgo del entorno surge de la existencia de fuerzas externas, tenemos por ejemplo dentro de este Riesgo los siguientes:
Riesgo Político: Acciones políticas adversas amenazan los recursos de la empresa y sus flujos de caja futuros en un país en que la empresa en cuestión ha invertido, o firmado un contrato que esté sujeta a leyes cambiantes.

II. RIESGOS DE PROCESOS

Es el riesgo que los procesos de negocios de la empresa no adquieren, no lo tienen definidos, o no están siendo operados de manera eficaz

Riesgos de operaciones
Es el riesgo de que sean ineficaces en la ejecución del modelo de negocio de la empresa.

Riesgo Proyecto; Se presenta cuando surgen inconvenientes dentro del marco de un proyecto (en su gestión) , que posiblemente lo conlleven al fracasa, generando pérdidas de diversos tipos, tanto económicos y de imagen.
Riesgo Técnico: Comprende los factores asociados con el desarrollo de determinados productos. Por ejemplo, los módulos de software que funcionan bien independientemente, fallan cuando se instalan en conjunto[34].

[33] Modelo de Riesgos de Negocios de Protiviti
[34] Estrategias y Tácticas en la Dirección y Gestión de Proyectos – Autor: Luis José Amendola.

Riesgos financieros

Es el riesgo que los flujos de caja y activos financieros no se manejan de manera efectiva, dentro de este rubro se encuentra el riesgo crediticio como el incumplimiento de las deudas pendientes.

Riesgos de dirección

Esta alineado a los riesgos del personal de la empresa, aquí se tocan temas de liderazgo, funciones entre otros.

Riesgos de tecnología de información

Riesgos asociados a la tecnología de información usada en la empresa, como cuando por ejemplo los sistemas no se están operando según lo planificado, o cuando perjudica la integridad de la información

Riesgo Funcionalidad; En el caso en que las funcionalidades de un sistema produzcan errores, ocasionando que se pierda la información, se procese información no íntegra o cualquier otro evento inconsistente.

Riesgos de integridad

Es el riesgo de fraude gerencial, fraude de personal, actos ilegales y actos no autorizados, los cuales podrían resultar en la pérdida de reputación en el mercado. (p.ej. Fraude Gerencial: Caso Enron).

III. RIESGOS DE INFORMACION PARA LA TOMA DE DECISIONES

El riesgo de información para la toma de decisiones es el riesgo de que la información utilizada no sea relevante o confiable. Estos riesgos se relacionan con todos los aspectos de las actividades de creación de valor de la empresa.

Riesgos de información operativa

Estos riesgos guardan relación con la falta de información para poder establecer ciertos parámetros (p. ej. Información para establecer los precios, o para firmar un contrato).

Riesgos de información de gestión

Ocurren con la ausencia de información financiera, contable, entre otros que no te ayuden a tener un panorama realista de la empresa.

Riesgos de información estratégica

Riesgos asociados a las decisiones de los directivos de la empresa.

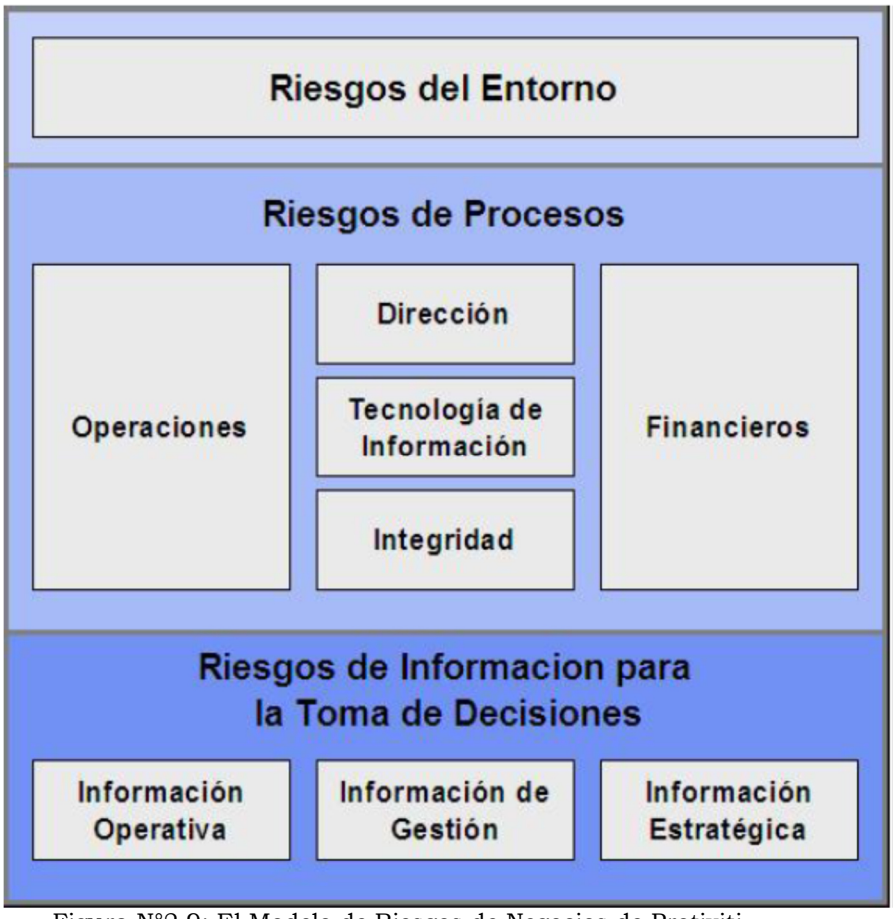


Figura N°2.9: El Modelo de Riesgos de Negocios de Protiviti

2.6.2 ESTRATEGIA DE COBERTURA DE RIESGOS

Para que el auditor tenga una visión clara al momento de evaluar el estado de los controles, debe tener la capacidad de identificar cuáles son las estrategias de cobertura que deben cubrir los controles sobre los riesgos. Estas estrategias pueden ser de 4 tipos:

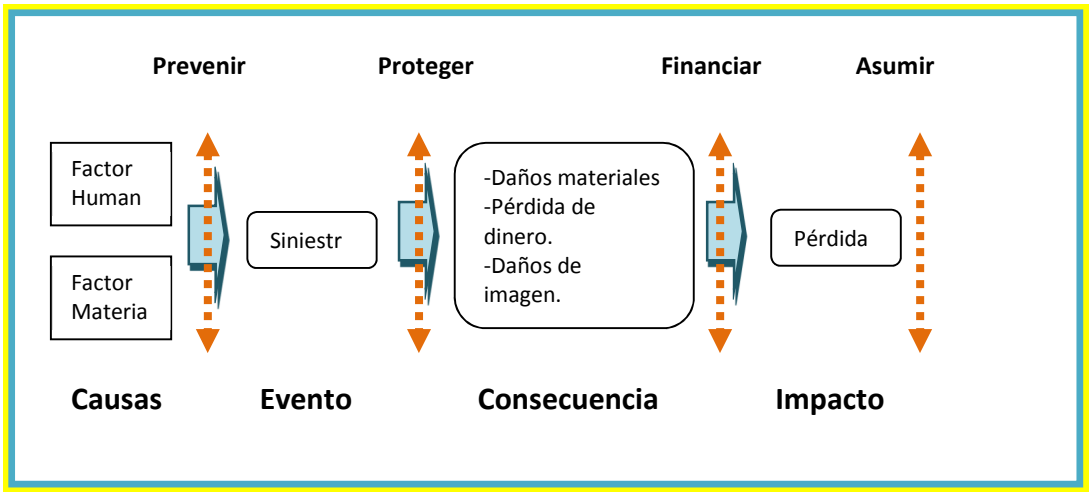


Figura N°2.10: Estrategia de cobertura de riesgos

Asumir el riesgo: Consiste en que la administración decidió no desarrollar ninguna acción para el control del riesgo evaluado. Esto implica que asumió el 100% de la consecuencia o impacto del riesgo. Los riesgos se asumen en la totalidad de su posible impacto ya sea porque el resultado de la evaluación muestra que las probabilidades de ocurrencia del evento asociado o sus consecuencias no son significativas; o porque al margen de ellas no se tiene recursos o no existen alternativas para efectuar una intervención.
La aceptación del riesgo es una decisión autónoma de la empresa, siempre y cuando no se violen preceptos legales existentes.

Financiar el riesgo: Consiste en controlar las consecuencias económicas de su posible impacto, estableciendo de manera previa los mecanismos para la financiación parcial, o total de pérdidas esperadas, ya sea con el uso de recursos propios o de terceros. Para ello se tiene dos alternativas:

a) Retener el riesgo.- Consiste en establecer una provisión real de fondos para responder a las pérdidas y garantizar la continuidad del negocio.

b) Transferir el riesgo.- Establecer acuerdos o condiciones contractuales para que en caso de ocurrir las consecuencias, un tercero asuma las posibles pérdidas. (Contratos de seguros o subcontratando). Básicamente la transferencia de riesgos es una herramienta de tipo financiero y es siempre una decisión gerencial.

Proteger o mitigar el riesgo: Consiste en actuar una vez producido el evento para limitar las consecuencias. La actuación sobre el evento mismo se denomina "Protección Activa", mientras que la acción limitadora de los efectos sin atacar el evento se conoce como "Protección Pasiva". Las medidas de protección incluyen, medios estructurales para el control o mitigación, sistemas y/o equipos de protección, procedimientos de acción, planes de emergencia y planes de contingencia.

Prevenir el riesgo: Consiste en actuar sobre el factor humano y materiales para disminuir las probabilidades de ocurrencia del evento.

Se debe diferenciar que mientras las medidas de prevención actúan sobre las amenazas o causas de riesgos disminuyendo las probabilidades de ocurrencia, las medidas de protección lo hacen sobre la vulnerabilidad limitando las consecuencias, y son por lo tanto dos variables independientes[35].

[35] Administración del Riesgo – Estándar Australiano/Neozelandés

CAPÍTULO III
ESTADO DEL ARTE

En el contexto de estudio de la presente tesina encontramos Normas, Marcos de Referencia, Estándares y otros, tales como la NTP ISO/IEC 17799:2007, el CobiT y el Estándar Australiano/Neozelandés/, los cuales nos proporcionan un marco referencial o modelo para gestionar riesgos.

Asimismo, presentamos las Metodologías que nos indican la forma de cómo realizar la gestión de riesgos, tal como MAGERIT y lo propuesto por el PMBOK del PMI.

También mostramos algunas técnicas y/o herramientas que nos permiten identificar las causas de riesgo, entre ellas tenemos al Diagrama de Afinidad, al Diagrama de Campo de Fuerzas, al Diagrama Causa-Efecto y la lluvia de ideas.

3.1 GESTIÓN DE RIESGOS

Para la gestión de los riesgos, existen una serie de Modelos como Normas, Estándares, y marcos de referencia, algunos de los principales definimos a continuación.

3.1.1 COBIT

Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT) brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. “Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a

optimizar las inversiones facilitadas por la TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien"[36].

El marco de trabajo general COBIT se presenta en un modelo de procesos compuesto de cuatro dominios que contienen 34 procesos genéricos, administrando los recursos de TI para proporcionar información al negocio de acuerdo con los requerimientos del negocio y de gobierno.

Los Dominios que considera son:

- Planear y Organizar
- Adquirir e implantar
- Entregar y Dar Soporte
- Monitorear y Evaluar

El Dominio "Planear y Organizar", se implementa a través de 10 objetivos de control, de los cuales, tomaremos en cuenta, para la presente tesina, el correspondiente a "Evaluar y Administrar Riesgos de TI".

A. EVALUAR Y ADMINISTRAR LOS RIESGOS DE TI

Este proceso permite crear y dar mantenimiento a un marco de trabajo de administración de riesgos que brindará estrategias de mitigación de riesgos.

Teniendo en cuenta cuales son las metas de la organización debemos identificar los eventos que puedan perjudicarlo, asimismo analizar y evaluar dichos eventos.

[36] CobiT - Control Objectives for Information and related Technology - Objetivos de control de información y tecnologías relacionadas

Para minimizar los riesgos a un nivel aceptable es necesario adoptar estrategias de mitigación de riesgos. El resultado de la evaluación debe ser entendible y se debe expresar en términos financieros, para que sea factible alinear los riesgos a un nivel aceptable de tolerancia.

Los objetivos de Control Detallados según CobiT son los siguientes:

Alineación de la administración de riesgos de TI y del negocio

Integrar la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización.

Establecimiento del contexto del riesgo

Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se aplica para garantizar los mejores resultados, incluyendo la determinación del contexto interno y externo de cada evaluación de riesgos, la meta y los criterios contra los cuales se evalúan los riesgos.

Identificación de eventos

Identificar todos aquellos eventos (amenazas y vulnerabilidades) con un impacto potencial sobre las metas o las operaciones de la empresa, aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operativos.

Asimismo se deberá determinar la naturaleza del impacto, verificar si tiene un nivel alto, medio o bajo, y mantener actualizado esta información.

IT Evaluación de riesgos

Evaluar de forma recurrente la posibilidad (frecuencia) e impacto (daños) de todos los riesgos identificados, usando métodos cualitativos y cuantitativos. La posibilidad e impacto asociados a los riesgos inherentes se debe determinar de forma individual, por categoría y basándose en el perfil de riesgos de la organización.

Respuesta a los riesgos

Identificar quienes son los propietarios de los riesgos identificados, así como también a los dueños de los procesos que se ven afectado con dichos riesgos, y elaborar y mantener respuestas a los riesgos que garanticen que los controles y las medidas de seguridad mitigan la exposición a los riesgos de forma continua.

La respuesta a los riesgos debe identificar estrategias de riesgo tales como evitar, reducir, compartir o asumir los mencionados riesgos, así también se debe considerar los costos y beneficios.

Mantenimiento y monitoreo de un plan de acción de riesgos

Planear las actividades de control asignando prioridades para implantar las respuestas a los riesgos, incluyendo la identificación de costos, beneficios y la responsabilidad de la ejecución. Buscar la aprobación para las acciones recomendadas y la aceptación de determinados riesgos, y asegurarse de que las acciones comprometidas las realicen los dueño (s) de los procesos afectados. Realizar seguimiento a la ejecución de los planes y reportar cualquier desviación a la alta dirección.

En resumen las actividades para la administración de Riesgos según CobiT son las siguientes:

1. Determinar la alineación de la administración de riesgos.

2. Entender los objetivos de negocio estratégicos relevantes.
3. Entender los objetivos de los procesos de negocio relevantes.
4. Identificar los eventos asociados con los objetivos de la organización.
5. Evaluar los riesgos asociados con los eventos.
6. Evaluar las respuestas de los riesgos.
7. Priorizar y planear las actividades de control.
8. Aprobar y garantizar el financiamiento de los planes de acción de riesgos.
9. Mantener y monitorear un plan de acción de riesgos.

3.1.2 NTP ISO/IEC 17799:2007 EDI: TECNOLOGÍA DE INFORMACIÓN: CODIGO DE BUENAS PRÁCTICAS PARA LA ADMINISTRACIÓN DE LA SEGURIDAD DE INFORMACIÓN.

Desde la publicación de la Resolución Ministerial Nº 244-2007-PCM, se obliga el uso de la NTP ISO/IEC 17799:2007, para la gestión de la seguridad de información en toda las Entidades integrantes del Sistema Nacional de Informática.

En el contenido de la ISO 17799, definen la Seguridad de Información, su importancia y la utilidad que representa en las organizaciones. Así como también establecen los requerimientos de seguridad de una empresa u organización, definiendo 3 aspectos para lograrlo:

"El primero consiste en evaluar los riesgos que enfrenta la organización. Mediante la evaluación de riesgos se identifican las amenazas a los activos, se evalúan las vulnerabilidades y probabilidades de ocurrencia, y se estima el impacto potencial.

El segundo aspecto está constituido por los requisitos legales, normativos, reglamentarios y contractuales que deben cumplir la organización, sus socios comerciales, los contratistas y los prestadores de servicios.

El tercer aspecto es el conjunto específico de principios, objetivos y requisitos para el procesamiento de la información, que ha desarrollado la organización para respaldar sus operaciones."[37]

Para la presente tesina nos enfocaremos en el primer aspecto o dominio, que es la Evaluación de Riesgos, y es definido en el Capitulo 4 de la Norma.

A. EVALUACION Y TRATAMIENTO DEL RIESGO

Evaluando los riesgos de seguridad

La evaluación de riesgos debe identificar, cuantificar y priorizar riesgos contra el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados deben guiar y determinar la apropiada acción de gestión y las prioridades para manejar la información de los riesgos de seguridad y para implementar controles seleccionados para proteger estos riesgos. El proceso de evaluación de riesgos y de seleccionar controles puede requerir que sea realizado un número de veces con el fin de cubrir diferentes partes de la organización o sistemas de información individuales.

La evaluación del riesgo debe incluir un alcance sistemático sobre la estimación de la magnitud del riesgo (análisis del riesgo) y sobre el proceso de comparar el riesgo estimado con el criterio para determinar el significado de los riesgos (valoración del riesgo).

Las evaluaciones del riesgo deben ser realizadas periódicamente para incluir los cambios en los requerimientos

[37] Norma NTP ISO/IEC 17799:2007

del sistema y en la situación del riesgo, por ejemplo en los activos, amenazas, vulnerabilidades, impactos, valoración del riesgo y cuando cambios significativos ocurran. Estas evaluaciones del riesgo deben ser emprendidas de una forma metódica, capaz de producir resultados comparables y reproducibles.

La evaluación de la información del riesgo de seguridad debe tener un alcance claro y definido para que este sea efectivo y debe incluir relaciones con las evaluaciones del riesgo en otras áreas, si es apropiado.

El alcance de la evaluación del riesgo puede ser para toda la organización, partes de ella, un sistema individual de información, componentes específicos del sistema o servicios donde esto puede ser utilizado, realista y provechoso. Ejemplos de metodologías de la evaluación del riesgo son discutidas en ISO/IEC TR 13335-3 (Guía para la gestión en la seguridad de tecnologías de información).

Tratando riesgos de seguridad

Antes de considerar el tratamiento de un riesgo, la organización debe decidir el criterio para determinar si es que los riesgos son aceptados o no. Los riesgos pueden ser aceptados si, por ejemplo, se evalúa que el riesgo es menor o que el costo de tratarlo no es rentable para la organización. Estas decisiones deben ser documentadas.

Para cada uno de los riesgos identificados, siguiendo la evaluación del riesgo, se necesita tomar una decisión del tratamiento del riesgo. Algunas opciones para el tratamiento del riesgo incluye:

a) Aplicar controles apropiados para reducir riesgos.

b) Riesgos aceptados objetivamente y con conocimiento, satisfaciendo claramente el criterio para la aceptación del riesgo y la política de la organización.
c) Evitar riesgos no permitiendo realizar acciones que puedan causar que estos riesgos ocurran.
d) Transferir los riesgos asociados a terceros como son los proveedores y aseguradores.

Para esos riesgos donde la decisión del tratamiento del riesgo ha sido aplicado a controles apropiados, esos controles deben ser seleccionados e implementados para conocer los requerimientos identificados por una evaluación de riesgos. Los controles deben asegurarse de que los riesgos son reducidos a un nivel aceptable tomando en cuenta:

a) Exigencias de las legislaciones y regulaciones nacionales e internacionales.
b) Objetivos organizacionales.
c) Exigencias operacionales.
d) Costo de la implementación y operación en relación con los riesgos que serán reducidos y siendo proporcional a las exigencias de la organización.
e) La necesidad de balancear la inversión en implementación y operación de los controles contra el daño que pueda resultar de las fallas en la seguridad.

Los controles pueden ser seleccionados de este estándar o de otro conjunto de controles o de nuevos controles que pueden ser designados para conocer las necesidades específicas de la organización.

Los controles en la seguridad de información deben ser considerados en los sistemas y en las especificaciones de las exigencias de los proyectos así como en la etapa de diseño. Las fallas pueden resultar en costos adicionales y en soluciones

menos efectivas y posiblemente, en el peor de los casos, inhabilidad para alcanzar una seguridad adecuada.

Se debe tener en cuenta que ningún conjunto de controles puede alcanzar completa seguridad y que una gestión adicional deberá implementarse para monitorear, evaluar y mejorar la eficiencia y efectividad de los controles de seguridad para apoyar las necesidades de la organización.

3.1.3 ADMINISTRACIÓN DE RIESGOS - ESTÁNDAR AUSTRALIANO/ NEOZELANDÉS

"Este estándar fue preparado por el Comité OB/7 de la junta de estándares de Australia y Nueva Zelanda sobre administración de riesgos como una revisión de AS/NZS 4360:1995 *Administración de riesgos.* De acuerdo a este se conserva el objetivo de proveer un marco conceptual genérico para el establecimiento del contexto, identificación, análisis, evaluación, tratamiento, monitoreo y comunicación del riesgo"

Del estudio del Estándar Australiano/Neozelandés[38] AS/NZS 4360:1999 identificamos los elementos principales de todo proceso de gestión integral o administración de riesgos, que son los siguientes:

[38] Éste estándar provee una guía genérica para el establecimiento e implementación del proceso de administración del riesgo involucrando la identificación, análisis, evaluación, tratamiento y monitoreo sobre la marcha de los riesgos.

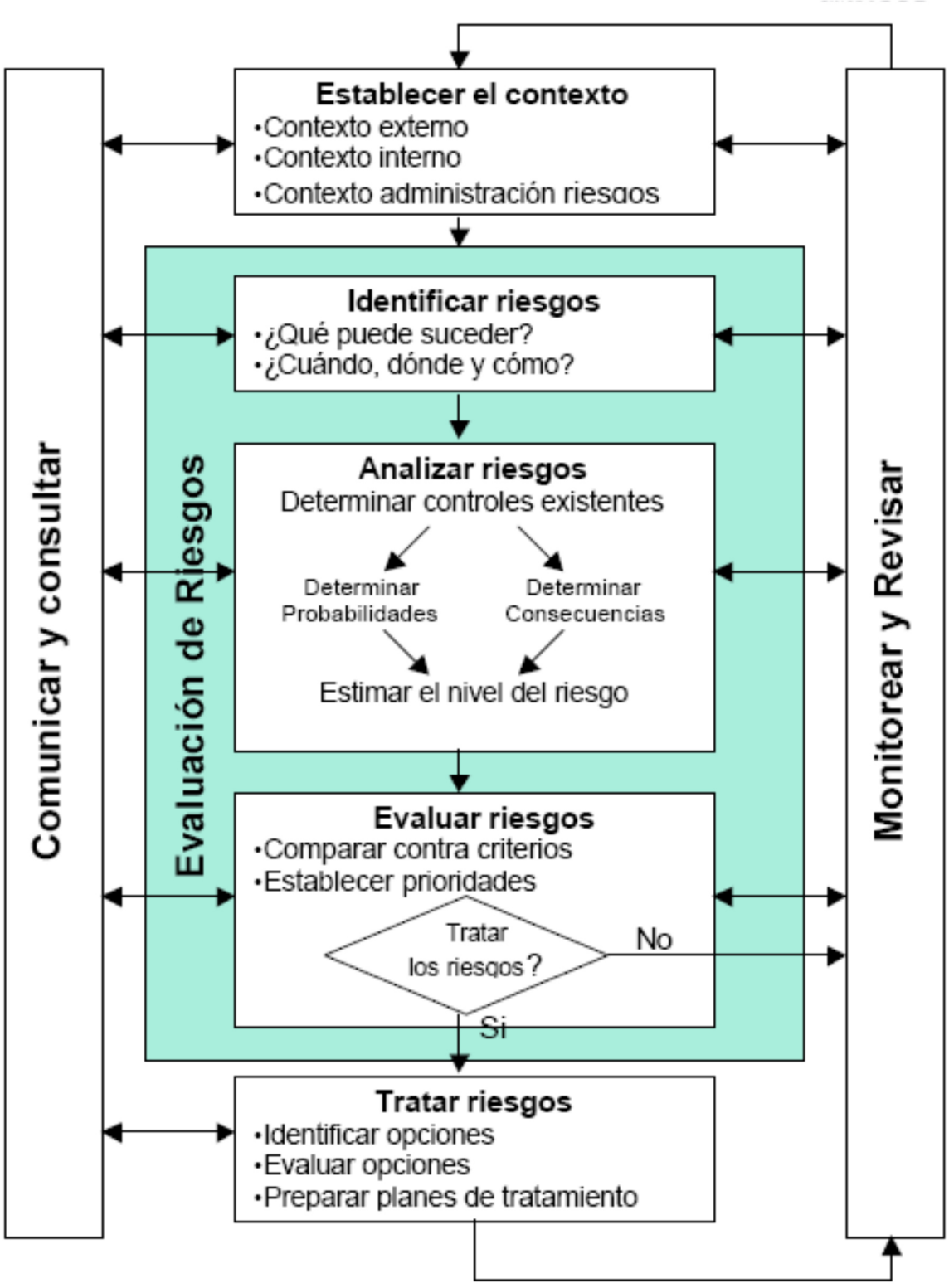


Figura N°3.1: Administración de Riesgos

Fuente: Estándar Australiano

A. ESTABLECER EL CONTEXTO

El proceso de administración de riesgos se produce dentro de la estructura del contexto estratégico, interno, externo y de administración de riesgos de una organización. Establecer el contexto consiste en definir los criterios o parámetros contra los cuales se evaluarán los riesgos y definir el alcance para el resto del proceso de la gestión del riesgo.

En el ámbito interno es indispensable conocer y comprender el funcionamiento de la organización, su estructura y capacidades, así como sus metas y objetivos estratégicos.

En el externo conocer su relación en torno a los aspectos de tipo de negocio, social, político, identificando sus fortalezas, debilidades, oportunidades y amenazas.
Para establecer el contexto de la administración de riesgos se deben establecer las metas, objetivos, estrategias, alcance y parámetros de la actividad, o parte de la organización al cual se está aplicando el proceso de administración de riesgos.

El proceso debería ser llevado a cabo con plena consideración a la necesidad de balancear costos, beneficios y oportunidades. También deberían especificarse los recursos requeridos y los registros a mantener.

B. IDENTIFICAR LOS RIESGOS

En esta fase se procura identificar el perfil de riesgos a ser administrados, incluyendo todos aquellos aspectos que estén o no bajo control en la organización El propósito además de identificar los riesgos según la naturaleza del negocio, es conocer las causas de riesgos.

El propósito es generar una lista amplia de fuentes riesgos y eventos para ello, es necesario considerar las causas y escenarios posibles.

Para este propósito se emplean diversas técnicas entre las cuales se tiene a los checklists, juicios de expertos, registros, diagramas de flujo, lluvia de ideas y análisis de escenarios.

C. ANALIZAR LOS RIESGOS

Esta etapa involucra considerar las fuentes de riesgo, sus consecuencias positivas o negativas y la probabilidad de que esas consecuencias puedan ocurrir. El riesgo se analiza combinando la probabilidad de que se presenten las causas de riesgos y sus consecuencias.

Para ello se determinan estrategias para comprobar los controles existentes, y dependiendo del tipo de información que se tenga, se pueda optar por un tipo de análisis cualitativos[39], o cuantitativo[40].

D. EVALUAR LOS RIESGOS

El objetivo de la evaluación de riesgos es tomar decisiones, basadas en los resultados del análisis de riesgo, acerca de los riesgos que requieren tratamiento y sus prioridades.

La evaluación de riesgos involucra comparar el nivel de riesgo detectado con los tipos de control de riesgo previamente establecidos. Las decisiones deben incluir consideraciones de tolerancia a los riesgos o si pueden ser tolerables.

[39] El análisis cualitativo utiliza formatos de palabras o escalas descriptivas para describir la magnitud de las consecuencias potenciales y la probabilidad de que ocurran esas consecuencias.
[40] El análisis cuantitativo utiliza valores numéricos (en lugar de las escalas descriptivas utilizadas en el análisis cualitativo) tanto para las consecuencias como para las probabilidades utilizando datos de una variedad de fuentes

Los riesgos bajos o tolerables podrían ser aceptados con un tratamiento futuro mínimo. Los mismos deberían ser monitoreados y revisados periódicamente para asegurar que se mantienen igual.

Si los riesgos no son tolerables, los mismos deberían ser tratados utilizando una o más de las opciones consideradas en el tratamiento de riesgos.

En algunas circunstancias, la evaluación de riesgos podría conducir a la decisión de llevar a cabo un mayor análisis.

E. TRATAR LOS RIESGOS

Involucra identificar y definir el rango de opciones que se debe adoptar para tratar los riesgos, preparando planes de tratamiento del riesgo e implementándolos.

F. COMUNICAR Y CONSULTAR

Es importante difundir en toda la organización una cultura de comunicación y consulta permanente sobre la gestión de los riesgos. Esto ayuda a que la gestión de riesgos contribuya al cumplimiento de los objetivos estratégicos del negocio.

G. MONITOREAR Y REVISAR

Los riesgos y la eficacia de las medidas de su tratamiento necesitan ser monitoreados en forma permanente para asegurar que se adapten a las condiciones cambiantes.

Podemos observar, después de leer el contenido de los acápites 3.1.1, 3.1.2 y 3.1.3 definen la gestión de riesgos de manera similar, es decir, nos proporcionan un marco general de referencia.

3.2 METODOLOGÍAS PARA GESTIONAR RIESGOS

A continuación tenemos algunas metodologías que nos indican la forma para realizar la gestión de riesgos, así tenemos la metodología MAGERIT y lo propuesto por el PMBOK del PMI.

3.2.1 MAGERIT

El Consejo Superior de Informática ha elaborado la Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones Públicas, MAGERIT, cuya utilización promueve, como respuesta a la dependencia creciente de éstas Tecnologías de la Información. La razón de ser de MAGERIT está pues directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero que también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que garanticen la autenticación, confidencialidad, integridad y disponibilidad de los sistemas de información y generen confianza cuando se utilicen tales medios[41].

La Metodología MAGERIT tiene un objetivo inmediato doble:

- Estudiar los riesgos que soporta un determinado sistema de información (SI) y el entorno asociable con él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio, en una primera aproximación que se atiene a la acepción habitual del término.

- Recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados.

[41] Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - MAGERIT

Para conseguir estos objetivos, MAGERIT tiene una estructura con dos tipos de elementos:

- Un conjunto de Guías, compuesto básicamente por:
    - Guía de Aproximación
    - Guía de Procedimientos
    - Guía de Técnicas
    - Guía para Desarrolladores de Aplicaciones
    - Guía para Responsables del Dominio protegible
    - Referencia de Normas legales y Técnicas.

- A Un panel de herramientas de apoyo, con sus correspondientes Guías de Uso y con la Arquitectura de información y especificaciones de la Interfaz para el intercambio de datos.

Esta estructura de MAGERIT permite realizar:

- El análisis de los riesgos para identificar las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el Sistema de información (conocidos como 'activos'); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.

- La gestión de los riesgos, basada en los resultados obtenidos en el análisis anterior, que permite seleccionar e implantar las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

En el capítulo 4 de la Metodología MAGERIT definen las etapas para realizar la gestión de riesgos, que se definen con detalle en los capítulo 6, 7, 8 y 9 de

la guía; a continuación presentamos un resumen de las etapas de la gestión de riesgos, según MAGERIT:

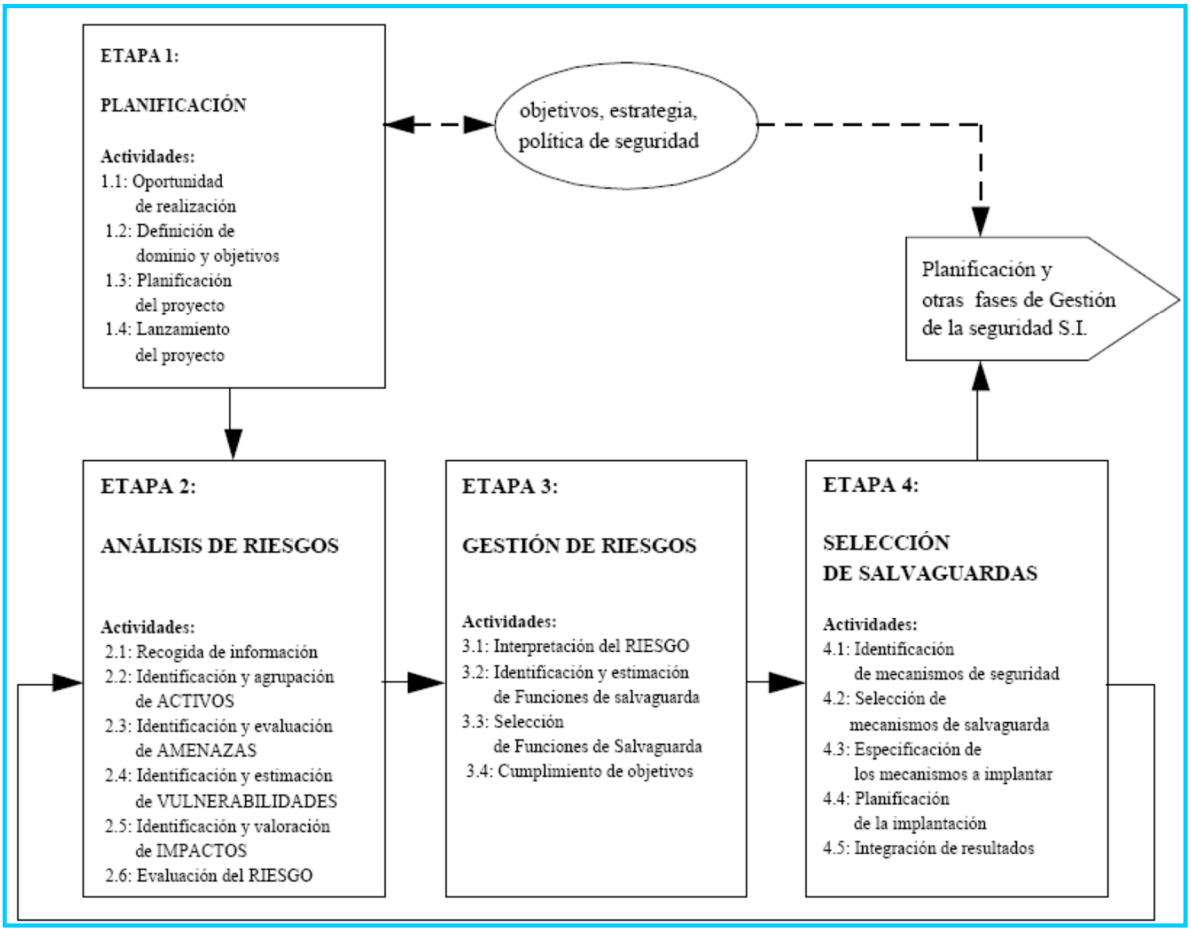


Figura 3.2: Gestión de Riesgos según MAGERIT

La figura anterior representa el Ciclo de Etapas (iterativo) del Proceso cubierto por MAGERIT que constituye la Fase de Análisis y Gestión de Riesgos dentro de la Gestión de la Seguridad de los Sistemas de Información. Asimismo se anotan los enlaces de este ciclo MAGERIT con la Fase de 'Objetivos, Estrategia y Política de Seguridad' (que es anterior y concomitante con MAGERIT) y con la Fase de 'Planificación de los Mecanismos de Salvaguarda' (que inicia el resto de la Gestión de la Seguridad).

ETAPA 1: PLANIFICACIÓN DEL ANÁLISIS Y GESTIÓN DE RIESGOS

La Etapa establece las consideraciones necesarias para arrancar el proyecto de análisis y gestión de riesgos; permite investigar la oportunidad de realizarlo; definir los objetivos que ha de cumplir y el dominio (ámbito) que abarcará; planificar los medios materiales y humanos para su realización; e iniciar el lanzamiento del proyecto MAGERIT define en esta Etapa de Planificación del proyecto de Análisis y Gestión de Riesgos las 4 actividades siguientes:

1. Oportunidad de realización

Se estudian los aspectos básicos para la realización de un proyecto de Análisis y Gestión de Riesgos, fundamentando la oportunidad de ésta. Se inicia una primera aproximación a los objetivos asignados al proyecto, al dominio -o ámbito- a incluir y a los medios necesarios para su elaboración.

2. Definición de dominio y objetivos

Se definen los objetivos finales del proyecto, su dominio y sus límites. Se realiza una primera identificación del entorno y de las restricciones generales a considerar. Se establecen los colectivos (responsables, técnicos, usuarios, etc.) a considerar para la recogida de información.

3. Organización y Planificación del proyecto

Se determina la carga de trabajo que supone la realización del proyecto y las características del grupo de trabajo a constituir. Se planifican las entrevistas a realizar para la recogida de información. Se establece quiénes son el resto de participantes, así como su modo de actuación. Se elabora el plan de trabajo para la realización del proyecto.

4. Lanzamiento del proyecto

Se adaptan los cuestionarios para la recogida de información en función al entorno retenido. Se eligen las técnicas principales de evaluación de riesgo a utilizar y se asignan los recursos necesarios para el comienzo del proyecto. También se realiza una campaña informativa de sensibilización a los afectados sobre las finalidades y requerimientos en su participación.

HITOS DE CONTROL

- La Dirección procederá a la aprobación o no de la realización del proyecto de Análisis y Gestión de Riesgos, basándose en el estudio de oportunidad realizado por el Promotor.
- El Comité Director del proyecto validará el informe de "Planificación del Análisis y Gestión de riesgos" que contendrá una síntesis de los productos obtenidos en las actividades realizadas en la Etapa.

RESULTADOS

Documentación intermedia

- Resultados de las entrevistas.
- Documentación de otras fuentes: estadísticas, observaciones de expertos y observaciones de los analistas.
- Documentación auxiliar: planos, organigramas, requisitos, especificaciones, análisis funcionales, cuadernos de carga, manuales de usuario, manuales de explotación, diagramas de flujo de información y de procesos, modelos de datos, etc.
- Análisis de los resultados, con la detección de las áreas críticas claves.
- Información existente utilizable por el proyecto (por ejemplo ,inventario de Activos)

- Resultados de posibles aplicaciones de métodos de Análisis y Gestión de Riesgos realizadas anteriormente (por ejemplo catalogación, agrupación y valoración de activos, amenazas, vulnerabilidades, impactos, riesgo, mecanismos de salvaguarda, etc.).

Documentación final

- Informe de "Planificación del Análisis y Gestión de riesgos" que contendrá una síntesis de los productos obtenidos en las actividades realizadas en la etapa.

ETAPA 2. ANÁLISIS DE RIESGOS

La Etapa permite identificar y valorar los elementos que intervienen en el riesgo; obtener una evaluación de éste en las distintas áreas del dominio; y estimar los umbrales de riesgo deseables.

1. ***Recogida de información***

   Obtención de la información sobre el sistema, de sus componentes, y de los factores que pueden influir en la seguridad.

2. ***Identificación y agrupación de ACTIVOS***

   Estudio detallado de la identificación, caracterización, interrelaciones, dependencias y valoraciones de los Activos en cuanto a su contribución a la evaluación del riesgo.

3. ***Identificación y evaluación de AMENAZAS***

Estudio detallado de la identificación, caracterización, interrelaciones, dependencias y valoraciones de las Amenazas en cuanto a su contribución a la evaluación del riesgo.

4. ***Identificación y estimación de VULNERABILIDADES***

Estudio detallado de la identificación, caracterización, interrelaciones, dependencias y valoraciones de las Vulnerabilidades en cuanto a su contribución a la evaluación del riesgo.

5. ***Identificación y valoración de IMPACTOS***

Estudio detallado de la identificación, caracterización, interrelaciones, dependencias y valoraciones de los Impactos en cuanto a su contribución a la evaluación del riesgo.

6. ***Evaluación del RIESGO***

Valoración del riesgo intrínseco y del riesgo efectivo, a partir de los resultados de las Actividades anteriores.

HITO DE CONTROL

- El Comité director debe establecer los umbrales de riesgo, definiendo el riesgo residual aceptable que se va a utilizar en la siguiente etapa, como medio para seleccionar las salvaguardas reductoras del riesgo al nivel elegido.
- La Dirección procederá a la aprobación o no de los resultados de la Etapa presentados por el Director del Proyecto.

RESULTADOS

Documentación intermedia

- Resultados de las entrevistas.
- Documentación de otras fuentes: estadísticas, observaciones de expertos y observaciones de los analistas.
- Documentación auxiliar: planos, organigramas, requisitos, especificaciones, análisis funcionales, cuadernos de carga, manuales de usuario, manuales de explotación, diagramas de flujo de información y de procesos, modelo de datos, etc.
- Resultados de la catalogación, clasificación y valoración de activos, de salvaguardas existentes, de amenazas, de vulnerabilidades, de impactos y del riesgo obtenido.
- Análisis de los resultados, con la detección de las áreas críticas claves.

Documentación final

- Riesgo global, riesgo distribuido por áreas, áreas críticas y umbrales de riesgo.

ETAPA 3. GESTIÓN DE RIESGOS

La Etapa permite identificar las posibles funciones o servicios de salvaguarda reductores del riesgo detectado; seleccionar las salvaguardas aceptables en función de las ya existentes y de las restricciones; simular diversas combinaciones; y especificar las finalmente elegidas.

1. ***Interpretación del riesgo***

   Interpretación de los resultados generados en las actividades anteriores, orientada a descubrir las principales áreas críticas.

2. ***Identificación de funciones de salvaguarda y estimación de su efectividad***

Identificación y estimación de la efectividad de las funciones o servicios de salvaguarda necesarias para reducir el riesgo a los umbrales aceptados.

3. Selección de las funciones de salvaguarda

Selección de las funciones o servicios de salvaguarda óptimos que cumplan los objetivos de reducción del riesgo.

4. Cumplimiento de objetivos

Estudio de los riesgos residuales obtenidos por la aplicación de las funciones o servicios de salvaguarda seleccionados, para determinar si se encuentran dentro de los umbrales de riesgo elegidos.

HITOS DE CONTROL

- El Comité director debe aprobar el conjunto de funciones y servicios de salvaguarda propuestos.
- La Dirección procederá a la aprobación o no de los resultados de la Etapa presentados por el Director del Proyecto.

RESULTADOS

Documentación intermedia

- Lista de funciones y servicios de salvaguarda ordenados según su efectividad, con una descripción de sus características.
- Informe de funciones y servicios de salvaguarda existentes, estimando su efectividad.
- Informe de funciones y servicios de salvaguarda seleccionados, con justificación de cada uno.
- Nuevos valores del riesgo al aplicar las funciones y servicios de salvaguarda propuestos

- Informe del estudio comparativo de resultados en las simulaciones.

Documentación final

- Lista final de funciones y servicios de salvaguarda propuestos.

ETAPA 4. SELECCIÓN DE SALVAGUARDAS

La Etapa permite seleccionar los mecanismos de salvaguarda a implantar; elaborar una orientación del plan de implantación de los mecanismos de salvaguarda elegidos; establecer los mecanismos de seguimiento para la implantación; recopilar los documentos de trabajo del proceso de Análisis y Gestión de Riesgos; obtener los documentos finales del proyecto; y realizar las presentaciones de los resultados a los diversos niveles

1. ***Identificación de los mecanismos***

   Se identifican de los mecanismos que puedan materializar las funciones y servicios de salvaguarda.

2. ***Selección de mecanismos de salvaguarda***

   Se seleccionan y estudian los mecanismos de salvaguarda anteriores que cumplan las restricciones y alcancen una efectividad suficiente en la reducción del nivel de riesgo.

3. ***Especificación de los mecanismos a implantar***

   La tarea especifica para los mecanismos de salvaguarda seleccionados ciertas características importantes.

4. ***Orientación a la planificación de la Implantación***

La priorización de los mecanismos seleccionados junto a la estimación de los recursos necesarios permiten realizar una aproximación a los cronogramas de implantación.

5. Integración de resultados

En esta actividad final se recopilan los informes de Etapa para generar el informe final y los documentos correspondientes para realizar presentaciones a diversos niveles.

HITOS DE CONTROL

- El Comité Director deberá aprobar el conjunto de mecanismos de salvaguarda propuestos para su implantación, los recursos necesarios que conlleven, así como el modo de dicha implantación.
- La Dirección procederá a la aprobación o no de los resultados de la Etapa presentados por el Director del Proyecto.

RESULTADOS

Documentación intermedia

- Documentos relativos a los mecanismos seleccionados y sus características, su modo de implantación y los recursos necesarios para ésta.

Documentación final

- Documento principal del trabajo realizado: "Informe final del Análisis y Gestión de Riesgos".

3.2.2 PMBOK: GUÍA DE LOS FUNDAMENTOS DE LA DIRECCIÓN DE PROYECTOS

La finalidad principal de la Guía del PMBOK es identificar el subconjunto de Fundamentos de la Dirección de Proyectos generalmente reconocido como buenas prácticas. “Identificar” significa proporcionar una descripción general en contraposición a una descripción exhaustiva. “Generalmente reconocido” significa que

los conocimientos y las prácticas descritos son aplicables a la mayoría de los proyectos, la mayor parte del tiempo, y que existe un amplio consenso sobre su valor y utilidad. “Buenas prácticas” significa que existe un acuerdo general en que la correcta aplicación de estas habilidades, herramientas y técnicas puede aumentar las posibilidades de éxito de una amplia variedad de proyectos diferentes. “Buenas prácticas” no quiere decir que los conocimientos descritos deban aplicarse siempre de forma uniforme en todos los proyectos; el equipo de dirección del proyecto es responsable de determinar lo que es apropiado para cada proyecto determinado. [42]

Para el estudio de la presente tesina tomamos el capítulo 11 del PMBOK, debido a que presentan una metodología de cómo realizar la gestión de riesgos de proyectos, utilizando las buenas prácticas.

CAPÍTULO 11: GESTIÓN DE RIESGOS DE PROYECTO

La Gestión de los Riesgos del Proyecto incluye los procesos relacionados con la planificación de la gestión de riesgos, la identificación y el análisis de riesgos, las respuestas a los riesgos, y el seguimiento y control de riesgos de un proyecto; la mayoría de estos procesos se actualizan durante el proyecto. Los objetivos de la Gestión de los Riesgos del Proyecto son aumentar la probabilidad y el impacto de los eventos positivos, y disminuir la probabilidad y el impacto de los eventos adversos para el proyecto. Los procesos de Gestión de los Riesgos del Proyecto incluyen lo siguiente:

[42] Guía de los Fundamentos de la Dirección de Proyectos.- PMBOK

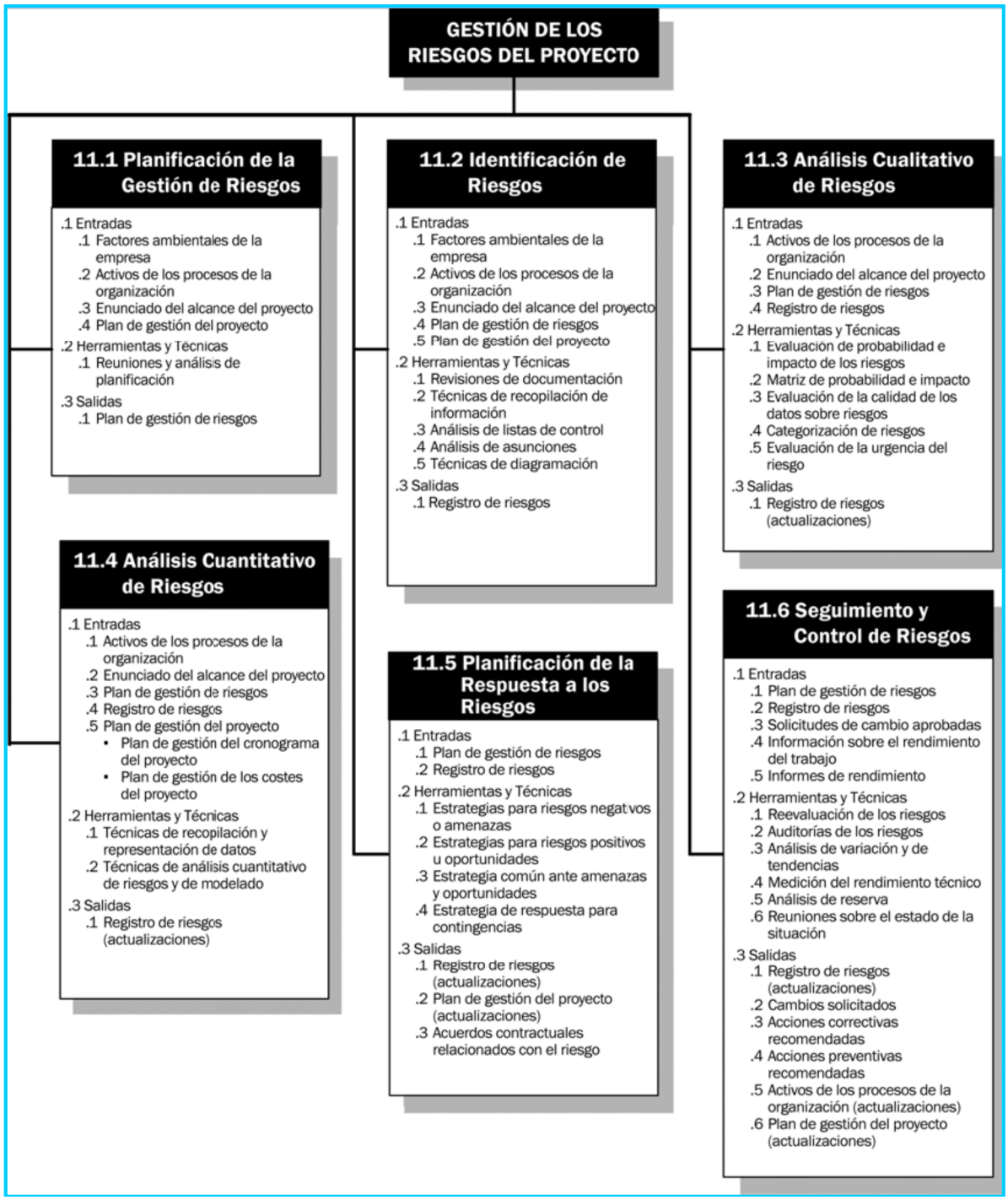


Figura 3.3 Descripción general de los procesos de Gestión de los Riesgos del Proyecto

A. PLANIFICACIÓN DE LA GESTIÓN DE RIESGOS

Una planificación cuidadosa y explícita mejora la posibilidad de éxito de los otros cinco procesos de gestión de riesgos. La Planificación de la Gestión de Riesgos es el proceso de decidir cómo abordar y llevar a cabo las actividades de gestión de riesgos de un proyecto. La planificación de los procesos de gestión de riesgos es importante para garantizar que el nivel, el tipo y la visibilidad de la gestión de riesgos sean acordes con el riesgo y la importancia del proyecto para la organización, a fin de proporcionar recursos y tiempo suficientes para las actividades de gestión de riesgos, y para establecer una base acordada para evaluar los riesgos. El proceso Planificación de la Gestión de Riesgos debe completarse en las fases tempranas de la planificación del proyecto, dado que es crucial para realizar con éxito los demás procesos descritos en este capítulo.

Entradas

- Factores Ambientales de la Empresa
- Activos de los Procesos de la Organización
- Enunciado del Alcance del Proyecto
- Plan de Gestión del Proyecto

Herramientas y Técnicas

- Reuniones de Planificación y Análisis

Salidas

Plan de Gestión de Riesgos; describe cómo se estructurará y realizará la gestión de riesgos en el proyecto. Incluye lo siguiente:

- Metodología.
- Roles y responsabilidades
- Preparación del presupuesto.
- Periodicidad.
- Categorías de riesgo.

- Matriz de probabilidad e impacto.
- Tolerancias revisadas de los interesados.
- Formatos de informe.
- Seguimiento.

B. IDENTIFICACIÓN DE RIESGOS

La Identificación de Riesgos determina qué riesgos pueden afectar al proyecto y documenta sus características. Entre las personas que participan en actividades de identificación de riesgos se pueden incluir, según corresponda, las siguientes: el director del proyecto, los miembros del equipo del proyecto, el equipo de gestión de riesgos (si se asigna uno), expertos en la materia ajenos al equipo del proyecto, clientes, usuarios finales, otros directores de proyectos, interesados y expertos en gestión de riesgos. Si bien estos miembros del personal son a menudo participantes clave de la identificación de riesgos, se debería fomentar la identificación de riesgos por parte de todo el personal del proyecto.

Entradas

- Factores Ambientales de la Empresa
- Activos de los Procesos de la Organización
- Enunciado del Alcance del Proyecto
- Plan de Gestión de Riesgos
- Plan de Gestión del Proyecto

Herramientas y Técnicas

- Revisiones de Documentación
- Técnicas de Recopilación de Información
- Análisis mediante Lista de Control
- Análisis de Asunciones
- Técnicas de Diagramación
    - Diagramas de causa y efecto

- Diagramas de flujo o de sistemas.
- Diagramas de influencias

Salidas

- Registro de Riesgos
  - Lista de riesgos identificados.
  - Lista de posibles respuestas.
  - Causas de riesgo
  - Categorías de riesgo actualizadas.

C. ANÁLISIS CUALITATIVO DE RIESGOS

El Análisis Cualitativo de Riesgos incluye los métodos para priorizar los riesgos identificados para realizar otras acciones, como Análisis Cuantitativo de Riesgos o Planificación de la Respuesta a los Riesgos. Las organizaciones pueden mejorar el rendimiento del proyecto de manera efectiva centrándose en los riesgos de alta prioridad. El Análisis Cualitativo de Riesgos evalúa la prioridad de los riesgos identificados usando la probabilidad de ocurrencia, el impacto correspondiente sobre los objetivos del proyecto si los riesgos efectivamente ocurren, así como otros factores como el plazo y la tolerancia al riesgo de las restricciones del proyecto como coste, cronograma, alcance y calidad.

Entradas

- Activos de los Procesos de la Organización
- Enunciado del Alcance del Proyecto
- Plan de Gestión de Riesgos
- Registro de Riesgos

Herramientas y Técnicas

- Evaluación de Probabilidad e Impacto de los Riesgos
- Matriz de probabilidad e impacto
- Evaluación de la Calidad de los Datos sobre Riesgos

- Categorización de Riesgos
- Evaluación de la Urgencia de los Riesgos

Salidas

- Registro de Riesgos (Actualizaciones)
  - Lista de prioridades o clasificaciones relativas de los riesgos del proyecto.
  - Riesgos agrupados por categorías.
  - Lista de riesgos que requieren respuesta a corto plazo.
  - Lista de riesgos que requieren análisis y respuesta adicionales.
  - Listas de supervisión de riesgos de baja prioridad.
  - Tendencias en los resultados del análisis cualitativo de riesgos.

D. ANÁLISIS CUANTITATIVO DE RIESGOS

El Análisis Cuantitativo de Riesgos se realiza respecto a los riesgos priorizados en el proceso Análisis Cualitativo de Riesgos por tener un posible impacto significativo sobre las demandas concurrentes del proyecto. El proceso Análisis Cuantitativo de Riesgos analiza el efecto de esos riesgos y les asigna una calificación numérica. También presenta un método cuantitativo para tomar decisiones en caso de incertidumbre. Este proceso usa técnicas tales como la simulación Monte Carlo y el análisis mediante árbol de decisiones para:

- Cuantificar los posibles resultados del proyecto y sus probabilidades
- Evaluar la probabilidad de lograr los objetivos específicos del proyecto
- Identificar los riesgos que requieren una mayor atención mediante la cuantificación de su contribución relativa al riesgo general del proyecto

- Identificar objetivos de coste, cronograma o alcance realistas y viables, dados los riesgos del proyecto
- Determinar la mejor decisión de dirección de proyectos cuando algunas condiciones o resultados son inciertos.

Entradas

- Activos de los Procesos de la Organización
- Enunciado del Alcance del Proyecto
- Plan de Gestión de Riesgos
- Registro de Riesgos
- Plan de Gestión del Proyecto

Herramientas y Técnicas

- Técnicas de Recopilación y Representación de Datos
- Técnicas de Análisis Cuantitativo de Riesgos y de Modelado
  - Análisis de sensibilidad.
  - Análisis del valor monetario esperado.
  - Análisis mediante árbol de decisiones.

Salidas

- Registro de Riesgos (Actualizaciones)
  - Análisis probabilístico del proyecto.
  - Probabilidad de lograr los objetivos de coste y tiempo.
  - Lista priorizada de riesgos cuantificados
  - Tendencias en los resultados del análisis cuantitativo de riesgos.

E. PLANIFICACIÓN DE LA RESPUESTA A LOS RIESGOS:

La Planificación de la Respuesta a los Riesgos es el proceso de desarrollar opciones y determinar acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto. Se realiza después de los procesos Análisis Cualitativo de Riesgos y Análisis Cuantitativo de Riesgos. Incluye la identificación y asignación de una o más personas

(el "propietario de la respuesta a los riesgos") para que asuma la responsabilidad de cada respuesta a los riesgos acordada y financiada.

La Planificación de la Respuesta a los Riesgos aborda los riesgos en función de su prioridad, introduciendo recursos y actividades en el presupuesto, cronograma y plan de gestión del proyecto, según sea necesario.

Entradas

- Plan de Gestión de Riesgos
- Registro de Riesgos

Herramientas y Técnicas

- Estrategias para Riesgos Negativos o Amenazas
  - Evitar.
  - Transferir.
  - Mitigar.
- Estrategias para Riesgos Positivos u Oportunidades
- Estrategia Común ante Amenazas y Oportunidades
- Estrategia de Respuesta para Contingencias

Salidas

- Registro de Riesgos (Actualizaciones)
- Plan de Gestión del Proyecto (Actualizaciones)
- Acuerdos Contractuales Relacionados con el Riesgo

F. SEGUIMIENTO Y CONTROL DE RIESGOS:

Las respuestas a los riesgos planificadas que están incluidas en el plan de gestión del proyecto se ejecutan durante el ciclo de vida del proyecto, pero el trabajo del proyecto debe ser supervisado continuamente para detectar riesgos nuevos o que cambien. El Seguimiento y Control de Riesgos es el proceso de identificar, analizar y planificar nuevos riesgos, realizar el

seguimiento de los riesgos identificados y los que se encuentran en la lista de supervisión, volver a analizar los riesgos existentes, realizar el seguimiento de las condiciones que disparan los planes para contingencias, realizar el seguimiento de los riesgos residuales y revisar la ejecución de las respuestas a los riesgos mientras se evalúa su efectividad. El proceso Seguimiento y Control de Riesgos aplica técnicas, como el análisis de variación y de tendencias, que requieren el uso de datos de rendimiento generados durante la ejecución del proyecto. El proceso Seguimiento y Control de Riesgos, así como los demás procesos de gestión de riesgos, es un proceso continuo que se realiza durante la vida del proyecto.

Otras finalidades del proceso Seguimiento y Control de Riesgos son determinar si:

- Las asunciones del proyecto aún son válidas.
- El riesgo, según fue evaluado, ha cambiado de su estado anterior, a través del análisis de tendencias.
- Se están siguiendo políticas y procedimientos de gestión de riesgos correctos.
- Las reservas para contingencias de coste o cronograma deben modificarse para alinearlas con los riesgos del proyecto.

Entradas

- Plan de Gestión de Riesgos
- Registro de Riesgos
- Solicitudes de Cambio Aprobadas
- Información sobre el Rendimiento del Trabajo
- Informes de Rendimiento

Herramientas y Técnicas

- Reevaluación de los Riesgos
- Auditorías de los Riesgos

- Análisis de Variación y de Tendencias
- Medición del Rendimiento Técnico
- Análisis de Reserva
- Reuniones sobre el Estado de la Situación

Salidas

- Registro de Riesgos (Actualizaciones)
- Cambios solicitados
- Acciones Correctivas Recomendadas
- Acciones Preventivas Recomendadas
- Activos de los Procesos de la Organización (Actualizaciones)
- Plan de Gestión del Proyecto (Actualizaciones)

3.3 HERRAMIENTAS PARA IDENTIFICAR Y ANALIZAR LOS RIESGOS

Para una adecuada administración de riesgos es vital, tanto su identificación como su análisis identificando las causas que la originan, la frecuencia con la que se presentan y el impacto que puede ocasionar en una determinada organización.

Por tal motivo en éste capítulo presentamos algunas técnicas o herramientas que usualmente se utilizan en áreas orientadas a la calidad, los cuales pueden ser aplicadas y facilitarán el análisis de riesgos, puedan estos ser riesgos de Seguridad de Información, de gestión, entre otros.

El uso de las herramientas dependerá del contexto en el que se encuentre la evaluación en una auditoría o de acuerdo a la realidad de la Organización.

Las herramientas o técnicas son muchas, entre ellas tenemos, el Diagrama de Afinidad, el Diagrama de Causa-Efecto, Diagrama de Campo de Fuerzas, Diagrama Matricial, Diagrama de Dispersión, y otros; a continuación las definimos:

3.3.1 DIAGRAMA DE AFINIDAD

Se deberá utilizar el diagrama de Afinidad cuando se quiere:

- Estructurar una cuestión larga y complicada.
- Desglosar una cuestión complicada en componentes fáciles de comprender.
- Obtener consenso sobre un asunto o situación.

Los pasos son los siguientes:

PASO 1: Enunciar el asunto o problema el cual se deberá trabajar.

Al principio de la sesión de afinidad:

- Establezca un límite de tiempo para la sesión, Generalmente, con 45 a 60 minutos es suficiente.
- Comience con un planteo claro y objetivo del problema o meta, en el que todo el mundo concuerde.

PASO 2: Generar ideas para el asunto en cuestión.

- Cada participante deberá generar ideas y anotarlas en tarjetas, hojas de papel autoadhesivas.
- Los términos de la idea deben ser enunciados concisamente en una a tres palabras. Debe anotarse una sola idea por tarjeta u hoja de papel.

PASO 3: Recoger las hojas autoadhesivas ya completadas.

- Recoger las tarjetas (u hojas autoadhesivas), mezclarlas y luego pegarlas en una superficie plana, de tal modo que todos los participantes puedan verlas.

PASO 4: Ordenar los papeles en grupos relacionados

- Organizar las ideas uniendo aquellas que guardan relación una de otras y separarlas por grupos. Las ideas similares se consideran de "afinidad mutua".
- Los integrantes deberán exponer sus ideas frente a los demás, aclarando las ideas poco precisas.

PASO 5: Crear un título o encabezamiento para cada grupo

- Identificar el grupo de ideas de acuerdo al área, actor o estrategia que le de identidad al conjunto.
- Superponer ideas que expresen exactamente lo mismo, sin eliminar tarjetas.

PASO 6: Preparar el diagrama de afinidad para presentación

- En una hoja de papel grande, pizarra o pared mostrar el análisis del problema con identificación de áreas, subprocesos o actores.
- Las tarjetas de los títulos se deberán colocar en la parte superior de cada grupo. [43]

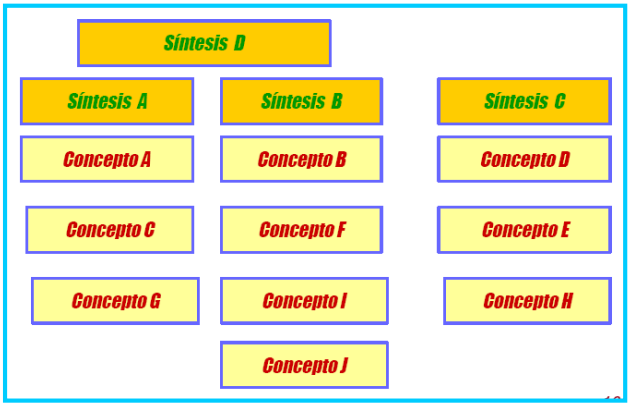


Figura 3.4: Diagrama de Afinidad

[43] ***Las Herramientas para la mejora continua de la calidad***- Autor: Richard Y. Chang, Matthew E. Niedzwiecki

3.3.2 DIAGRAMA DE CAMPO DE FUERZAS

El Diagrama de Campo de Fuerzas es una herramienta que el equipo utiliza cuando:

- Se está tratando de alcanzar un objetivo.
- Se está tratando de identificar las causas posibles y las soluciones a un problema o a una oportunidad importante.
- El equipo está atascado en la obtención de su objetivo.

El Diagrama de Campo de Fuerzas es para ser usado por grupos pequeños, entre 5 y 7 integrantes de personas que trabajan en un objetivo común.

PASO 1: Aprestarse para la sesión de Diagrama de Campo de Fuerzas.

Al inicio de la sesión de Campo de Fuerzas:

- Cree un gráfico como el indicado a continuación en un block o en una transparencia para proyectar.

Figura 3.5: Diagrama de Campo de Fuerzas

- Establezca un límite para la sesión, que puede durar entre 30 y 50 minutos.
- Designe uno o más registradores, cuya tarea consistirá en anotar en el diagrama las fuerzas aceleradoras y las frenadoras a medida que estas vayan apareciendo.

PASO 2: Ponerse de acuerdo sobre la situación corriente.

- La situación corriente se refiere a lo que está sucediendo actualmente y que uno no quiere cambiar o mejorar. Esto es siempre una cuestión corriente que necesita ser resuelta. Anote tal situación corriente en el Diagrama de Campo de Fuerzas.
- Si usted está al tanto de la situación corriente, lo más probable es que tenga también una idea sobre su objetivo. Discuta con su grupo cuál debería ser el objetivo. Llegue a un acuerdo sobre el objetivo, y anótelo en el diagrama de Campo de Fuerzas.

Figura 3.6: Diagrama de Campo de Fuerzas con objetivos

PASO 3: Determinar las fuerzas aceleradoras y las frenadoras.

- Las fuerzas aceleradoras son las cosas (acciones, conocimientos, equipos, procedimientos, cultura, gente, etc) que contribuyen a dirigirlo hacia su objetivo. Las fuerzas frenadoras son las cosas que tienden a impedir que alcance su objetivo.
- Como grupo se deberán hacer la siguiente pregunta: ¿Cuáles son las cosas que nos conducen hacia nuestro objetivo?
- El registrador debería anotar las respuestas en el lado izquierdo del Diagrama de Campo de Fuerzas. Las respuestas son anotadas a medida que se enuncian, dejando espacio entre cada respuesta. Esto continúa hasta que se hayan registrado todas las fuerzas.
- Luego planteé la pregunta: ¿Qué es lo que nos está impidiendo alcanzar nuestro objetivo?
- El Registrador anota entonces las respuestas en el lado derecho del Diagrama de Campo de Fuerzas. Otra vez, las respuestas se añoran a medida que se enuncian, dejando espacio entre cada respuesta. Continúe esto hasta que se hayan registrado todas las respuestas, y es así como obtenemos el Diagrama de Campo de Fuerzas. [44]

3.3.3 DIAGRAMA DE CAUSA-EFECTO

En 1953, el profesor Kaoru Ishikawa, de la Universidad de Tokio, cuando intentó clasificar y vincular las diferentes causas que influían sobre la calidad en la acería de Kawasaki, ideó el llamado Diagrama de Causa-Efecto, también denominado Diagrama de Ishikawa o de Espina de pescado. Posteriormente, este sencillo método se extendió por toda la industria japonesa primero y mundial después.[45]

Para poder entender mejor la naturaleza del diagrama de causa-efecto o también conocido como Diagrama de Ishikawa, citamos a continuación una serie de características:

[44] ***Las Herramientas para la mejora continua de la calidad***- Autor: Richard Y. Chang, Matthew E. Niedzwiecki
[45] ***Control estadístico de la Calidad-*** Autor Vicente Carot Alonso

- *Impacto visual, m*uestra las interrelaciones entre un efecto (materialización del riesgo) y sus posibles causas de forma ordenada, clara, precisa , debido a que la forma del gráfico es de fácil entendimiento para el lector.
- *Capacidad de comunicación, m*uestra las posibles interrelaciones causa-efecto permitiendo una mejor comprensión del fenómeno en estudio, incluso en situaciones muy complejas.
- *Centra la atención de todos los componentes del grupo en un problema específico de forma estructurada y sistemática.*

Sugerencias para elaborar los diagramas de causa-efecto

Identifique todos los factores relevantes mediante consulta y discusión entre muchas personas.

- Exprese la característica tan correctamente como sea posible
- Haga un diagrama para cada característica
- Escoja una característica y unos factores medibles
- Descubra factores sobre los que sea posible actuar. [46]

Sugerencias para el uso

- Asigne la importancia de cada factor objetivamente con base en datos
- Trate de mejorar continuamente el diagrama causa-efecto mientras lo usa

Utilidad de un diagrama de causa efecto

Los diagramas de causa efecto se construyen para ilustrar con claridad las diversas causas que afectan ella calidad del producto, clasificándolas y vinculándolas entre sí. Entre sus usos más importantes se encuentran:

- Retroalimenta la visión de cada uno de los involucrados.
- Guía de la discusión.

[46] ***Las Herramientas para la mejora continua de la calidad***- Autor: Richard Y. Chang, Matthew E. Niedzwiecki

- Definir diligentemente las causas y consignar los resultados.
- Reúne datos (orienta la adopción de las mediadas pertinentes)
- Pone de manifiesto el nivel de tecnología (revela un conocimiento acabado del proceso de producción).
- Es aplicable a cualquier tipo de problema.
- Permite visualizar de manera profunda el problema con sus causas.

Los pasos para realizarlo, son los siguientes:

PASO 1: Aprestarse para la sesión de Causa –Efecto

- El equipo deberá tener un número de entre 5 y 7 integrantes, y se deberá tener una pizarra o un papel donde todos puedan participar cuando se empiece a realizar el diagrama.

PASO2: Identificar el efecto.

- El efecto se refiere a la cuestión (problema o condición del proceso) que uno está tratando de modificar. Anote el efecto en el casillero del lado derecho diagrama de causa y efecto.

PASO 3: Identificar las principales categorías de causa.

- Identificar las causas principales que inciden sobre el efecto. Éstas serán las ramas principales del diagrama y constituirán las categorías bajo las cuales se especificarán otras posibles causas.
- Las categorías habitualmente usadas son las siguientes:
    - 3 Ms 1P: Maquinaria, Materiales, Métodos y Personal.
    - 4Ps: Personas, Políticas, Procedimientos y Planta.
    - Medio; Como una categoría potencialmente utilizable y que se refiere al entorno en que se lleva a cabo el proceso.

- Sin embargo, no es imprescindible utilizar estos grupos de categorías. Para cada problema, u objetivo, se definirán las que se consideren más relevantes en cada caso.
- Situar cada categoría de causa en sendos recuadros conectados con la línea central. Mediante un conjunto de líneas inclinadas. [47]

PASO4: Generar ideas sobre las causas potenciales del problema.

- Identificar, para cada rama principal, otros factores específicos que puedan ser causa del efecto. Tales factores conformarán las ramas de segundo nivel, éstas a su vez pueden expandirse en otras de tercer nivel, y así sucesivamente.
- Para esta expansión recurrente, será útil emplear series de preguntas iniciadas como: **porqué**. Asimismo, para desplegar las ramas se podrá usar lluvia de ideas.
- El número de niveles no tiene límites.

PASO 5: Revisar cada categoría principal de causa.

- Al concluir el diagrama, se deberá repasar para asegurar que se han incluido en él todos los factores causales posibles, así como también quitar causas que se consideren innecesarias, esto se dará por consenso.

[47] ***Pensar: tarea esencial de líderes y Gerentes,*** Autor: Luis Castañeda Martinez

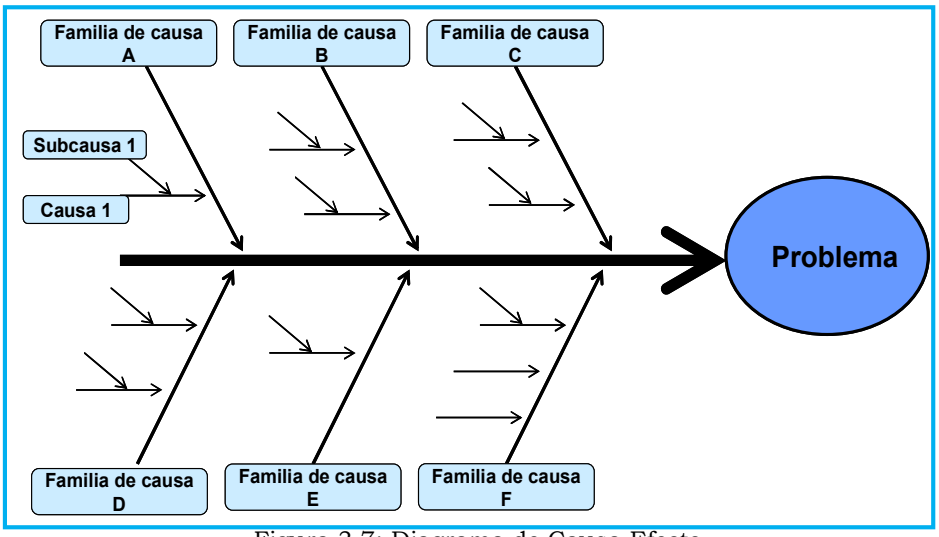


Figura 3.7: Diagrama de Causa Efecto

Fuente: Guía para la evaluación del Desempeño con Indicadores (Documento de la Contraloría General de la República)

3.3.4 LLUVIA DE IDEAS

La lluvia de ideas es una herramienta de creatividad bastante empleada en el trabajo de grupo, y en la que en un equipo genera y clarifica una lista de ideas. Se basa en una idea que da lugar a otra, y a otra, hasta que el grupo consigue tal riqueza de información que pueda pasar a la fase siguiente:

Algunos aspectos importantes de la lluvia de ideas:
- Se utiliza para crear un gran número de ideas.
- Es un esfuerzo creativo.
- Se utiliza en varios pasos del proceso de resolución de ideas.
- Es una herramienta simple pero muy efectiva.
- Es un mecanismo para promover la participación.

Los pasos para establecerlo son los siguientes:

PASO 1: Calentamiento

En la que el grupo ejercita para alcanzar un mejor funcionamiento colectivo y para activar las interconexiones neuronales propias del proceso creativo. Por ejemplo, se podrían nombrar todas las cosas que nos podríamos poner de sombrero.

PASO 2: Generación de ideas

En la que se establece un número mínimo de ideas al que se quiere llegar y se marca el tiempo durante el que se va a trabajar. En esta fase existen cuatro reglas fundamentales:

- Toda crítica está prohibida
- Toda idea es bienvenida
- Tantas ideas como sea posible
- El desarrollo y asociación de ideas es deseable

PASO 3: Trabajo con las ideas

Las ideas existentes pueden mejorarse mediante la aplicación de una lista de control. Con cada idea se deberían formular las siguientes preguntas:

- ¿Se puede aplicar de otro modo?
- ¿Se puede modificar?
- ¿Se puede ampliar?
- ¿Se puede reducir?
- ¿Se puede sustituir?
- ¿Se puede reorganizar?
- ¿Se puede invertir?
- ¿Se puede combinar?

PASO 4: Variar la forma de trabajo

Una vez se han pasado estas fases se hace una pausa para pulir las ideas seleccionadas

- El trabajo del grupo es complementado y/o sustituido por el trabajo individual o por contactos intergrupales
- La comunicación verbal es complementada y/o cambiada por comunicación escrita
- La reunión de ideas sin valoración es interrumpida por fases de valoración
- El comienzo sin ideas ya existentes es modificado mediante un inicio con un "banco de ideas"
- La reunión constructiva de estímulos es complementada por una compilación destructiva de desventajas
- La integración espontánea de ideas puede ser complementada y/o sustituida por una integración sucesiva
- La lista de control puede ser complementada y/o cambiada por estímulos visuales

PASO 5: Evaluación

Tras la generación de ideas, el grupo establece los criterios con los cuales va a evaluar las ideas. Por ejemplo: Rentabilidad económica, grado de factibilidad, grado de extensión de la idea[48]

3.4 APLICACIÓN DEL DIAGRAMA CAUSA-EFECTO PARA IDENTIFICAR LOS PRINCIPALES RIESGOS EN EL PLANEAMIENTO DE UNA AUDITORÍA DE PROCESOS

Los pasos a seguir para realizar la planificación de una auditoría de procesos aplicando al Diagrama de Causa-Efecto para identificar y analizar riesgos son:

3.4.1 DISEÑAR EL PROCESOS AUDITABLE

[48] Manual de Trabajo en equipo- Autor: Robert Winter

En general, el ejercicio de diseñar el proceso le permite al auditor levantar una primera hipótesis de los principales puntos de atención al momento de identificar los riesgos.

Pero para esto es necesario conocer el objetivo del proceso, y tener conocimientos de la importancia que tiene tal proceso dentro de su organización.

La auditoría de procesos tiene como meta principal efectuar las diferentes revisiones de auditoría a una determinada parte del proceso del negocio.

La finalidad del diseño del proceso auditable y alcance se orienta a cumplir con los objetivos de control interno en las actividades de dicho proceso[49] de negocio.

El desarrollo de este trabajo tiene como soporte base el trabajo en equipo así como a la técnica de entrevistas o cuestionarios con el personal involucrado. La recopilación de información es una etapa importante antes de efectuar las entrevistas.

A. FLUJOGRAMAR EL PROCESO AUDITABLE

El diseño será realizado por el equipo auditor utilizando como formato los procedimientos y los flujogramas definidos por la organización, así como también se deberá utilizar la información recogida de las entrevistas con los auditados, de tal forma que refleje la realidad del proceso.

[49] Los procesos siempre pueden sufrir alteraciones buscando mejorar las actividades dentro de la organización, a esto se le llama reingeniería de Procesos.

Se recomienda emplear el diagrama de flujo en **bloque**, que proporciona una visión general bastante rápida del proceso.

Los rectángulos y las líneas con flechas son los principales símbolos en el diagrama de bloque, representado el rectángulo a Los subprocesos y actividades, y las líneas conectan la dirección de ellas. Los círculos alargados señalan el inicio y fin de un proceso, tal como lo vemos en la siguiente figura.

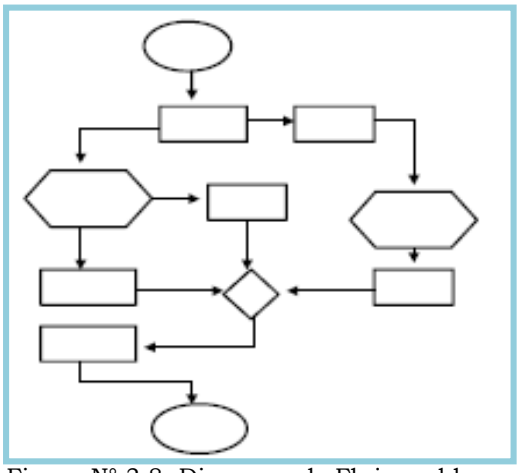
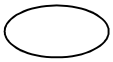


Figura N° 3.8: Diagrama de Flujo en bloques

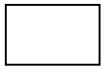
Tal representación gráfica requiere una descripción secuencial y puede ir acompañado de una serie de gráficas con mayor detalle para un mejor entendimiento del funcionamiento del proceso.

Mmostramos a continuación los principales símbolos que se usan para crear un diagrama de flujo.

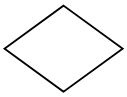


Inicio/Final: Linderos o fronteros del proceso. Define el input y output del proceso.

Subproceso: Partes bien definidas de un proceso con vinculación secuencial.

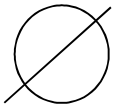


Actividad: Es la suma de tareas normalmente agrupados por un procedimiento.



Decisión: Condición para seguir el análisis del proceso.

Dirección: Hacia donde se dirige una decisión o sigue una secuencia.

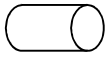


Actividad de control: Tareas vinculadas a la comprobación o validación de la ejecución de las operaciones o servicios.

Operaciones manuales: Constituye la realización de una operación o actividad en forma específicamente manual.

Almacenamiento de acceso secuencial: Se refiere a diskettes, cintas, cartuchos o medios que puede ser entrada o salida de información.

Documento: Referido a algún impreso o reporte obtenido de los sistemas informáticos.



Almacenamiento de acceso directo: Se refiere a la información que se guarda en los servidores de archivos o algún lugar donde se tiene acceso directo.

Archivo físico: Documento de datos.

Secuencia: Indica secuencia de diagramación de gráficos o flujos.

3.4.2 IDENTIFICAR LOS RECURSOS Y ACTIVIDADES CRÍTICAS DEL PROCESO

Una vez que ya tenemos el diagrama de flujo, procedemos a evaluarlo en conjunto con el equipo auditor, e identificar en el mismo diagrama las actividades que podrían verse afectadas ante la ocurrencia de

algún tipo de riesgo, asimismo podemos identificar los recursos críticos y los listamos.

Una vez que ya tenemos la lista de recursos críticos, y ya identificamos las actividades que podrían verse afectadas ante un riesgo, podemos realizar una **lista preliminar de riesgos**.

3.4.3 IDENTIFICAR LAS AMENAZAS O CAUSAS DE RIESGOS EN EL PROCESO

Obtenida una relación preliminar de los posibles riesgos que afectarían al proceso auditable, se procede a descomponer cada uno de ellos utilizando la herramienta que podemos considerar apropiada; como por ejemplo la técnica causa – efecto que con ayuda de la Lluvia de ideas, puede resultar eficiente para la labor de identificación de causas de riesgos.

A continuación mostramos el diagrama de causa efecto para la siguiente actividad:

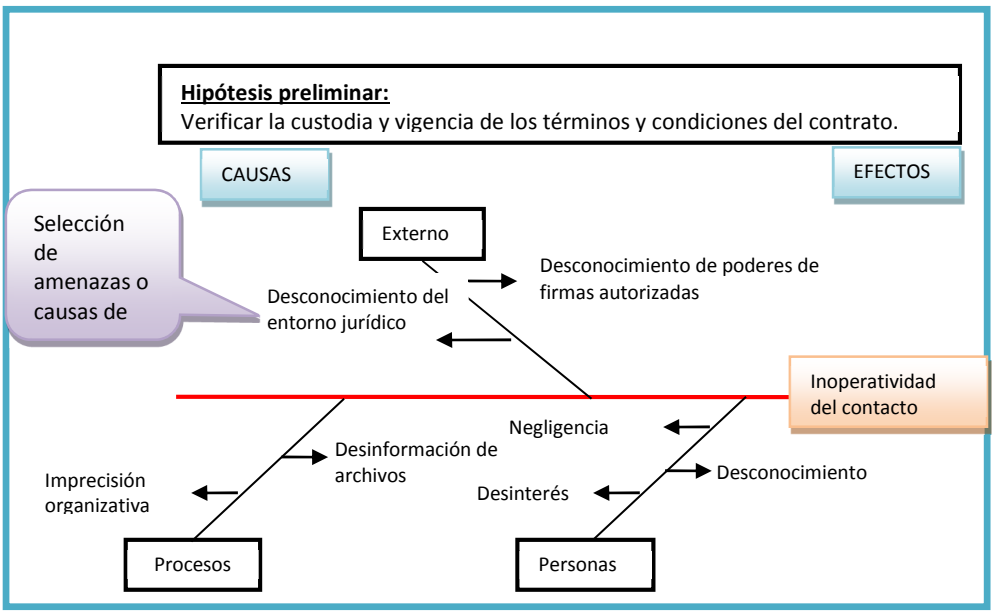


Figura N°3.9: Ejemplo de um Diagrama Causa-Efecto

A. EL DIAGRAMA CAUSA - EFECTO

Para poder encontrar las posibles causas de riesgos el equipo auditor deberá reunirse y explotar sus sugerencias mediante la técnica conocida como "Lluvia de ideas", ya definida en el acápite 3.3.4, esto es, cada auditor, basado en su experiencia, deberá sugerir causas que puedan desencadenar un determinado riesgo; y así, al obtener una lista de causas de riesgo.

Los pasos para aplicar el análisis causa - efecto lo hemos definido en el acápite 3.3.3, pero estos deben de adaptarse a la situación, en este caso tenemos como objetivo identificar las causas de los riesgos que se puedan presentar en el proceso auditable.

PASO 1. Definir, sencilla y brevemente, el problema o riesgo identificado en la etapa anterior (diagrama de flujo).

Como en la etapa anterior identificamos los posibles riesgos a ocurrir en el proceso, en este paso solo procedemos a colocarlo dentro de un rectángulo a la derecha de la superficie de escritura y dibujar una flecha, que corresponderá al eje central del diagrama, de izquierda a derecha, apuntando hacia él.

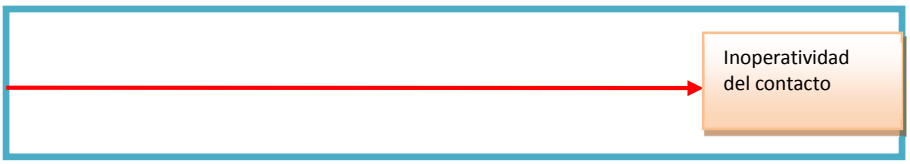


Figura N° 3.10: Ubicación del efecto

PASO 2. Identificar las posibles causas de riesgos principales o amenazas que ocasionan la existencia del efecto y agruparlos.

Como describimos al inicio, la lluvia de ideas nos ayudarán a identificar las amenazas o causas de riesgo, y agruparlos de acuerdo a su origen, podremos agruparlos en 4 grandes niveles que son los siguientes:

- Personas
- Tecnologías
- Procesos
- Externo

Estos niveles, pueden variar de acuerdo a lo que decida cada equipo auditor, y es adaptable a cada tipo de evaluación.

A continuación tenemos una tabla donde definiremos las posibles categorías para el Diagrama de Causa-Efecto que puede escoger el equipo auditor:

Categorías	Evento/Riesgo
Naturales	- Fenómenos naturales
Sociopolíticas	- Delincuencia, conflicto armado, social o terrorismo
Normativas	- Vicios en la Gestión - Inestabilidad legal
Comerciales	Incumplimiento de contrato
Económicas	- Factores Macroeconómicos
Dirección	-Incumplimiento o falta de alineación de la estrategia - Falta de oportunidad y calidad en la toma de decisiones.
Procesos	- Inadecuado flujo y calidad de información. - Falla humana - Falla de procesos
Sistemas y equipos	- Indisponibilidad de Hardware, software y otros equipos

Entorno/Externo	- Manejo de comunidades - Relaciones con accionistas

Tabla 3.1 : Categoría de Eventos

Posteriormente podremos seguir con la construcción del diagrama, y cada uno de estos grupos se deberán colocar en un rectángulo y conectarlos a la línea central.

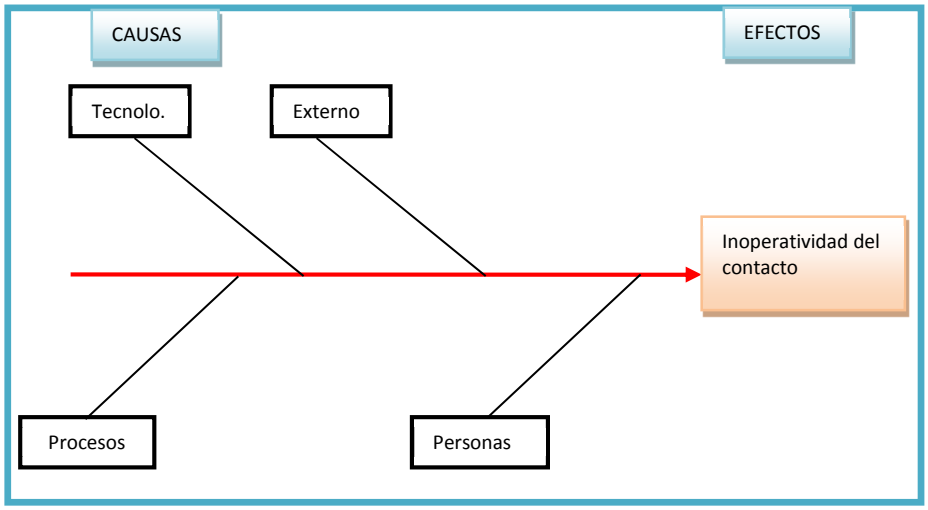
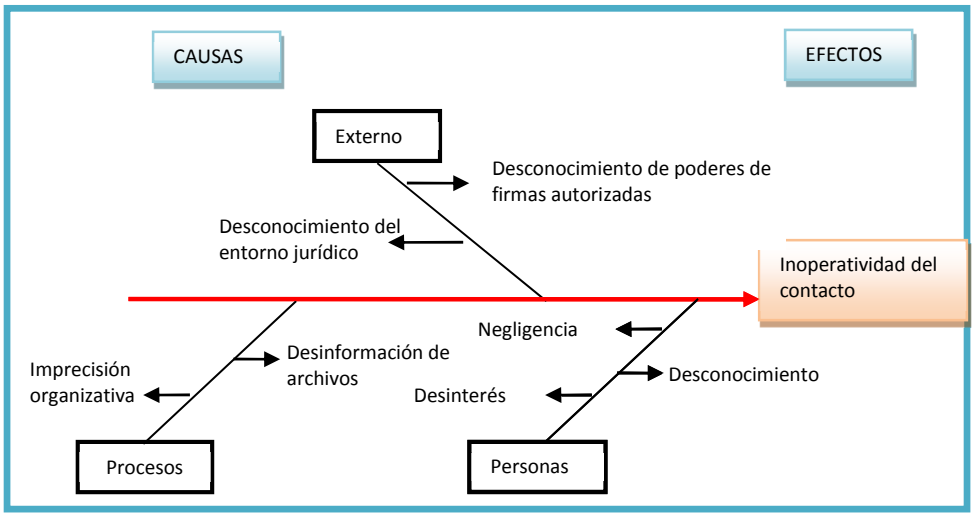


Figura N° 3.11: Ubicación de las causas de Riesgo

PASO 3.Añadir causas para cada rama principal.

Se continúa con la lluvia de ideas definiendo causas o amenazas de riesgo, y se escribe las más precisas en líneas perpendiculares que se unan a las barras de la causa de mayor nivel, según sea el caso, para ello es necesario que el equipo auditor tenga claro el proceso auditable dentro de la organización, sus entradas y salidas, estos datos le brindarán un mejor marco de referencia a los auditores para identificar con mayor claridad las causas de riesgos.

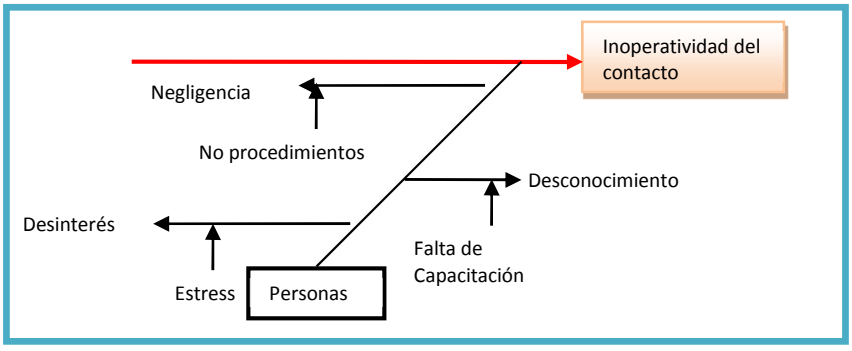
Figura N° 3.12: Añadiendo causas a las ramas.



PASO 4. Añadir causas subsidiarias para las subcausas anotadas, si es que es necesario.

Se deberá conectar líneas adicionales a las causas correspondientes según sea el caso, esto es si cada causa de riesgo presenta otras causas más detalladas.

Figura N° 3.13: Añadiendo causas subsidiarias.



PASO 5. Revisar cada categoría de Causa

Si no existe consenso obvio en las amenazas que ameritan mayor revisión, se usa alguna clase de votación con el fin de incrementar las oportunidades de éxito.

B. LISTAR LOS RIESGOS Y SUS CAUSAS DE RIESGO

Una vez depuradas las amenazas o causas de riesgo que se obtuvieron del diagrama de Causa-efecto se deberá seleccionar las más importantes según el criterio del equipo auditor.

	RIESGO/EFECTO	CAUSA DEL RIESGO	CATEGORÍA	
R1	Problemas en la ejecución de tareas.	Inadecuada disponibilidad de recursos humanos para ejecutar los procesos.	Personas	Recursos Humanos
		Falta de conocimientos, habilidades o actitudes de personalidad.	Personas	Recursos Humanos
R2	Incumplimiento en la estructura laboral.	Falta de manual de Procedimientos	Procesos	Eficiencia
R3	Inadecuado flujo de información	Falta de un sistema integral.	Tecnología	Infraestructura

Tabla N°3.2: Lista de Amenazas

Este inventario de riesgos, mediante su codificación y clasificación, facilitará el análisis al momento de construir el mapa de riesgos.

3.4.4 ANALIZAR LOS RIESGOS

Para un eficiente análisis de riesgos, utilizamos métricas, que nos permitirán medir ciertos atributos de los riesgos, en este caso necesitamos medir la probabilidad de ocurrencia y el impacto que tendría en la organización en caso se activara. Después de obtener los resultados de la medición de las causas del riesgo, procedemos a mapearlo.

A. MÉTRICAS PARA LA DEFINICIÓN DE LOS RIESGOS

- Definición de métrica en el análisis de riesgos dentro de una auditoría de procesos.

Una métrica o magnitud se define como "una medida cuantitativa de ciertos atributos que posee un proceso o su descomposición".

La métrica o magnitud en un proceso auditable es la aplicación permanente de medición de ciertas característica que posee un proceso o su descomposición, es decir en las actividades o tareas. En el caso particular del auditor, deben satisfacer las necesidades de conocer las magnitudes del mencionado proceso y de permitir construir tablas que permitan la evaluación de los riesgos encontrados.

Entre los beneficios de las métricas está que nos proporcionan información para decidir, de acuerdo a su complejidad y materialidad, que parte de los componentes auditables pueden tomar mayor tiempo en su evaluación.

Utilizamos métricas para efectuar el análisis de riesgos detectados en el proceso, con las cuales medimos la frecuencia o probabilidad con la que se puede presentar un determinado riesgo, así como identificar la consecuencia o impacto que pueda ocasionar al materializarse dicho riesgo, para ello es indispensable construir tablas vinculadas a la característica del proceso.

- Pasos para medir la frecuencia o probabilidad de los riesgos.

1. Definir la escala de las frecuencias o probabilidad de ocurrencia del riesgo y elaborar la tabla según la información disponible sobre el proceso.

2. El equipo por consenso selecciona la definición de los criterios según las escalas.

Un ejemplo de escala de medición de riesgo puede ser calificado del 1 al 5 como se indica en la siguiente tabla. Pueden ser de escalas menores o mayores por consenso, siempre que se permita facilitar su evaluación.

TABLA DE FRECUENCIA/PROBABILIDAD DE RIESGOS **Formato : Casos (Sucesos o incidentes) x tiempo**		
VALOR	**NIVEL**	**DEFINICIÓN DE CRITERIOS**
5	Constante	Más de 20 casos al año
4	Permanente	Entre 10 y 20 casos al año
3	Moderado	Entre 1 y 10 casos al año
2	Ocasional	1 caso entre 1 y 6 años
1	Improbable	1 caso entre 6 y 12 años

Tabla N° 3.3: Tabla de Frecuencia/Probabilidad de Riesgos

3. En el mismo sentido, se construye una escala de tablas para medir las consecuencias o vulnerabilidad de llegar a materializarse el riesgo, en montos o valores vinculados al proceso. También es libre la designación de niveles. En la siguiente tabla utilizamos 6 niveles para clasificarlo. (1, 2, 3, 4, 5, 6).

TABLA DE CONSECUENCIAS **Formato : Economías internas**		
VALOR	**NIVEL**	**DEFINICIÓN DE CRITERIOS**
1	Insignificante	Menos de S/. 5 000

2	Marginal	Entre S/.5 000 y 50 000
3	Grave	Entre S/.50 000 y 200 000
4	Crítico	Entre S/. 200 000 y 1 millón
5	Desastroso	Entre 1 millón y 5 millones
6	Catastrófico	Mas de S/. 5 millones

Tabla N°3.4: Tabla de Consecuencias

4. Conocido el proceso y su descomposición, así como las magnitudes o métricas de la materia auditable. Los riesgos identificados en forma preliminar antes de ir al trabajo de campo, son aquellos necesarios para evitar que se ponga en peligro la consecución de los objetivos del proceso.

B. MAPEANDO LOS RIESGOS

Obtenido la lista de riesgos conjuntamente con las métricas y magnitudes del mismo y el diagnóstico adquirido hasta el momento, se da inicio al mapeo de los riesgos.

Se utiliza para esta tarea un **mapa estándar de riesgos.** Cualquiera sean los valores de medición utilizados en las tablas se requiere establecer un "Patrón" o mapa de referencia único aplicable a cualquier tipo de análisis de riesgo independiente a su origen.

Estos mapas permiten visualizar el resultado de los diversos escenarios de frecuencia/probabilidad de los riesgos que podrían afectar al proceso.

La probabilidad es la herramienta para el "manejo de la incertidumbre" en el análisis de riesgos, ya que mide la "expectativa" de obtener un resultado posible:

Podemos emplear cualquiera de los tres tipos de probabilidad:

- *Estructural:* Probabilidad de que salga un evento según el número de opciones.
- *Frecuentista:* Análisis frecuencial de eventos.
- *Subjetiva:* Basada en opinión de expertos.

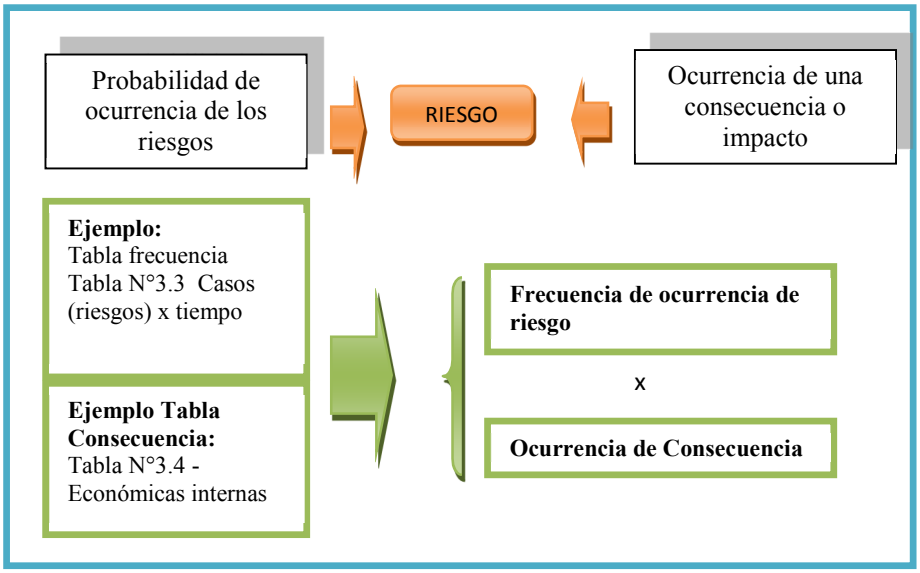


Figura N°3.14: Análisis de Riesgo, para la elaboración del Mapa de Riesgos.

Éste análisis se realiza necesariamente con apoyo de las tablas construidas para medir frecuencias/probabilidad de las amenazas y consecuencias.

En síntesis, el análisis de riesgo consiste en medir las tablas de frecuencias/probabilidad de los riesgos y de las consecuencias.

- ***Pasos para realizar la Matriz de Riesgos:***

a) Se empieza a crear el mapa de riesgos dibujando las coordenadas y las abscisas, ubicando en ellas los niveles identificados en las tablas de frecuencia/probabilidad de los riesgos (Tabla N° 3.6) y la

Tabla de Consecuencias (Tabla N°3.7), como lo observamos en la Figura N°3.14.

b) Luego se procede a ubicar en el mapa de riesgos los niveles de las tablas seleccionadas para conocer el grado en el cual los eventos potenciales podrían afectar el logro de los objetivos. Esta valorización de los eventos se hace desde la perspectiva de la frecuencia/probabilidad de los riesgos y consecuencias.

c) Finalmente procedemos a ubicar los riesgos dentro de la matriz, y se coloca su grado, que resulta de multiplicar los niveles correspondientes a la frecuencia de amenazas y consecuencias correspondientes.

Figura N°3.15: Matriz de Riesgos

El resultado del análisis de riesgos según los escenarios de frecuencia/probabilidad y consecuencias determinan el mapa de riesgos del proceso. Aquellos riesgos graficados en la zona de mayor peligro serán empleados como los más sensibles a los cuales se tiene que enfocar el programa de auditoría, dejando de lado aquellos que según su análisis, están controlados o considerados dentro de la zona de seguridad.

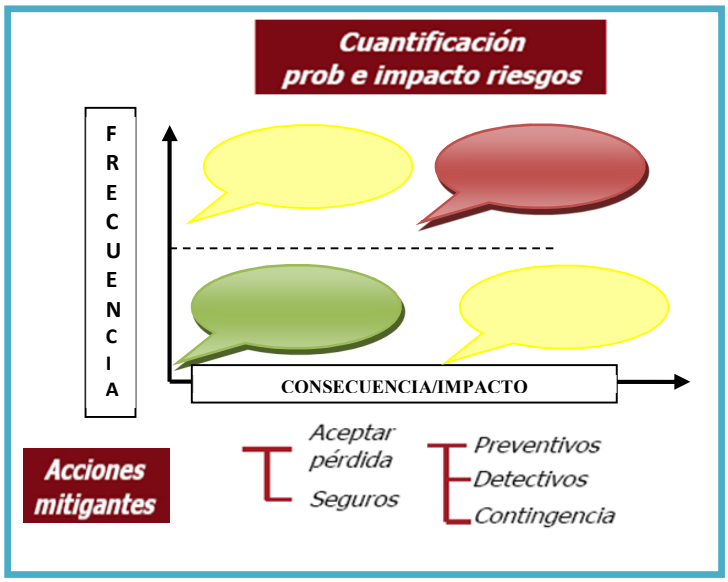


Figura N°3.16: Mapa de Riesgos

El resultado final de este proceso de análisis la identificación de los puntos de atención vinculados a los riesgos ubicados en la zona más sensibles sobre los que debe recaer prioritariamente el programa de auditoría a ejecutar.

CAPÍTULO IV

CASO PRÁCTICO

De acuerdo a los puntos elaborados en el capítulo anterior, acápite 3.4 primero identificamos el proceso a auditar, y a través del Diagrama de Causa-Efecto identificamos las causas de riesgo, listándolos y evaluándolos para su respectivo análisis.

Es importante tomar en cuenta la necesidad de que los auditores deberán tener conocimientos de procesos y riesgos y la gestión de los mismos.

Para el caso práctico tenemos al Proceso de Otorgamiento de Créditos a Entidades de un determinado Banco. Para mayor entendimiento del Caso, llamaremos a la Organización en cuestión como "El Banco".

4.1. DISEÑAR EL PROCESO "OTORGAMIENTO DE CRÉDITOS A ENTIDADES"

Antes de diseñar el proceso Primero definiremos su objetivo.

Objetivo Principal: Evaluar, aprobar o proponer al nivel correspondiente las solicitudes de créditos autorizadas. Asimismo, administrar adecuadamente la cartera de créditos, monitorear las colocaciones

El tema de Colocaciones para el Banco representa uno de los principales rubros en la generación de sus ingresos, razón por la cual es de mucha utilidad una evaluación a dicho proceso, identificando sus riesgos , que a su vez permitan mayor dinamismo y efectividad de sus actividades**.**

Es importante tomar en cuenta, que si el Banco le da mayor agilidad al proceso de otorgamiento de créditos a entidades, podrá incrementar su

capacidad operativa que a su vez, puede traducirse en un incremento del nivel de sus colocaciones. Razón por la cual debe realizar en forma paralela, **la implementación de mejoras tecnológicas y de infraestructura a los temas referidos a cobranzas y recuperaciones**, especialmente en la automatización de las labores de registro y seguimiento de operaciones de recupero de créditos, que permitan un adecuado control de la morosidad.

A. FLUJOGRAMAR EL PROCESO

A continuación mostramos el diagrama de flujo-jerárquico del Proceso Otorgamiento de Crédito a entidades.

Proceso: Otorgamiento de Créditos

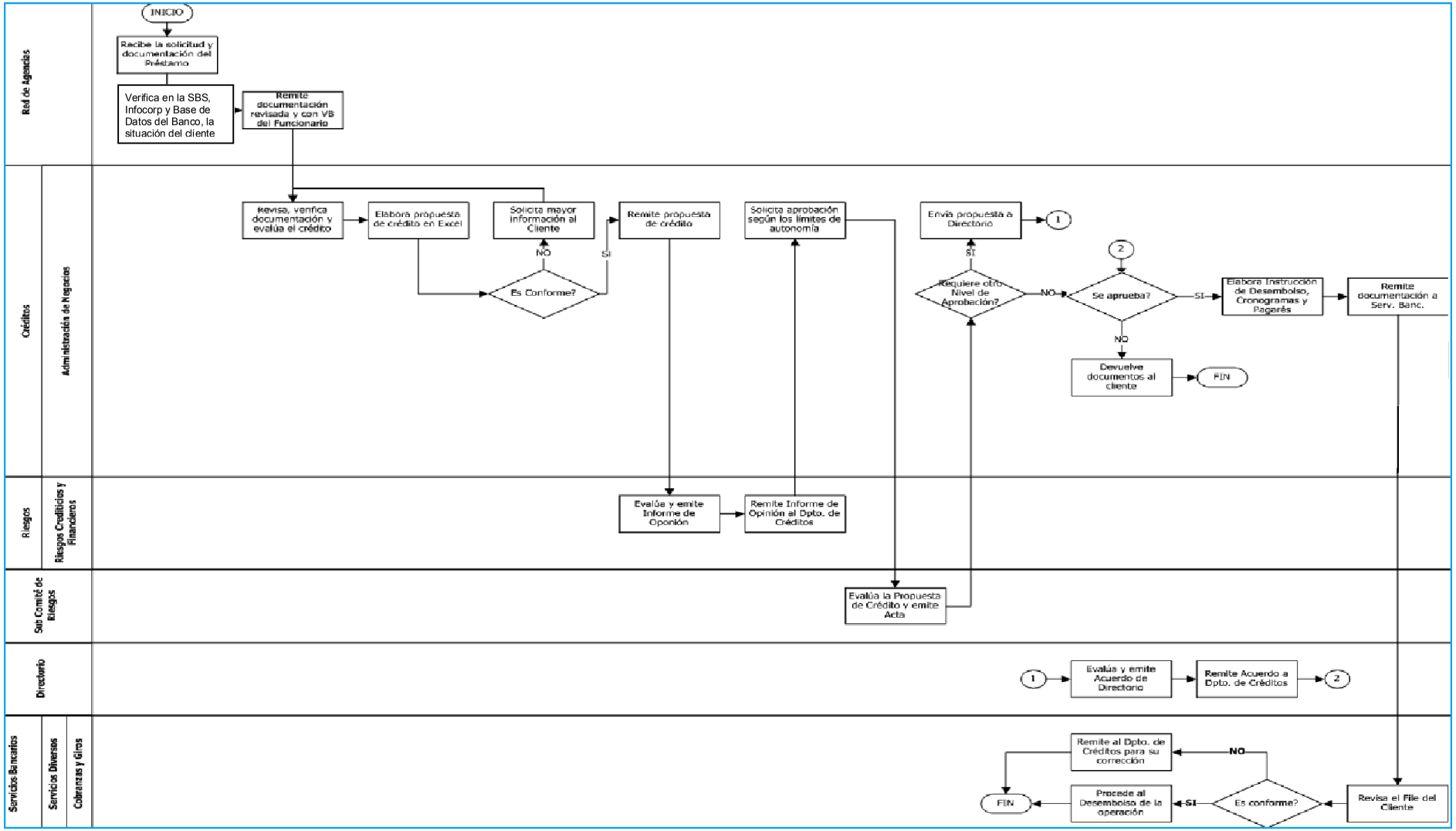


Figura N°4.1: Flujograma del Proceso Otorgamiento de Créditos a entidades

4.2 IDENTIFICAR LOS RECURSOS Y ACTIVIDADES CRÍTICAS DEL PROCESO:

Identificamos las actividades que podrían verse afectadas por algún tipo de riesgo, esta tarea se debe realizar de manera conjunta con todo el equipo auditor.

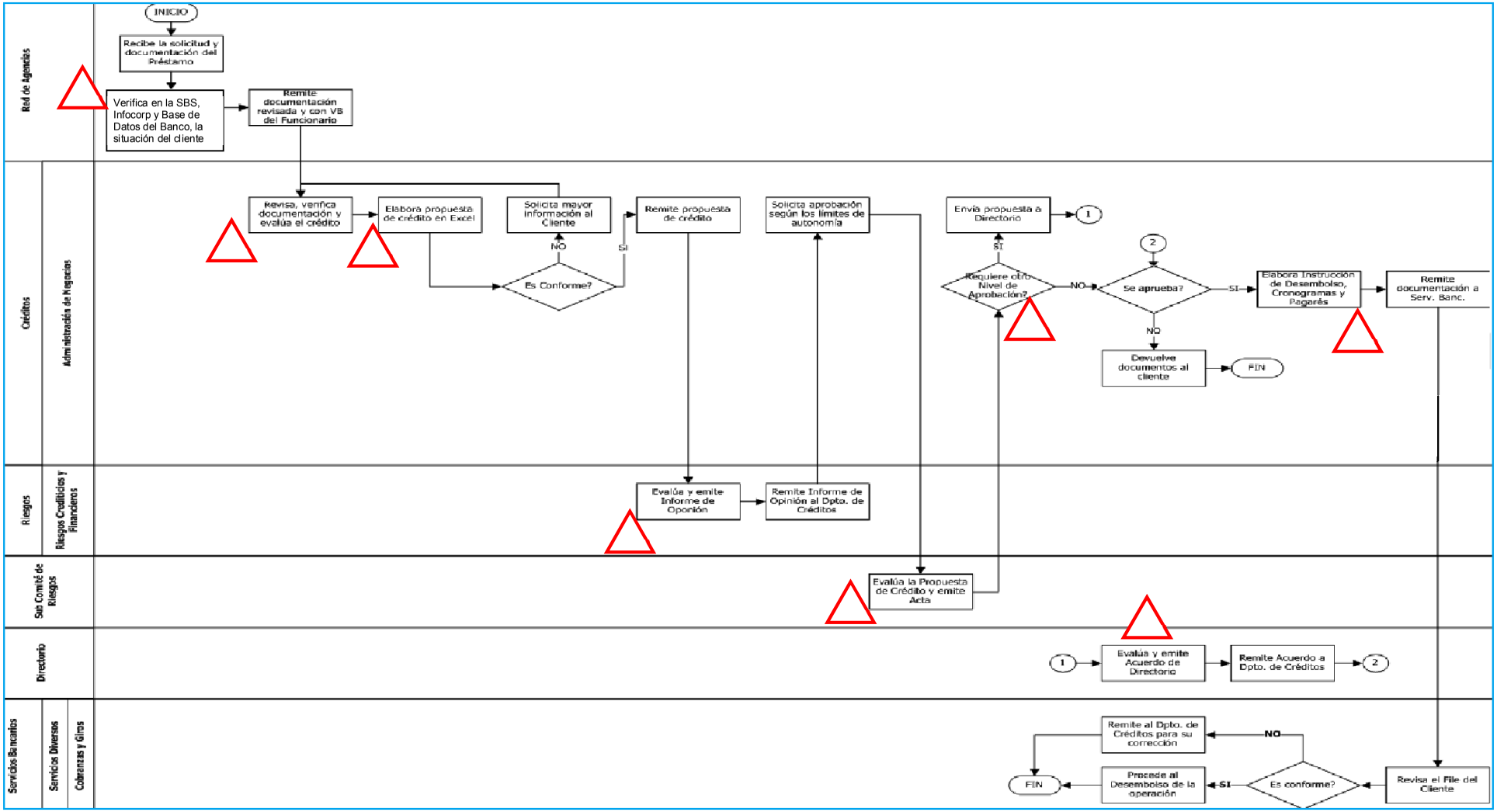


Figura N°4.2: Flujograma de Riesgos del Proceso Otorgamiento de Créditos a Entidades

Identificar los recursos críticos del proceso

Después de la identificación de las actividades críticas del diagrama de flujo del proceso de Otorgamiento de Créditos a Entidades, se pudo identificar los recursos críticos.

A continuación listamos los recursos críticos identificados:

- Personal:
  - del Dpto. Red de Agencias: Ejecutivo de Crédito
  - del Dpto. de Crédito: Evaluador de Créditos.
  - del Dpto. de Riesgos: Analista de Riesgos Crediticios y Financieros.
  - Miembros del Sub-Comité de Riesgos.
  - Miembros del Directorio.
- Sistemas:
  - Sistema de Infocorp
  - Sistema de la SBS- Superintendencia de Banca y Seguros
  - Sistema de PRAH: Donde se registran los créditos aprobados con sus respectivas características ().
  - Sistema de Propuesta de Créditos (Excel).
  - Sistema de Cronograma de Pagos (Excel).

Identificando los posibles riesgos del Proceso

- Caída del Sistema de Infocorp/SBS/PRAH
- Recepción de documentos falsos.
- Errores en la propuesta de crédito.
- Ineficiente análisis de riesgo crediticio.
- Créditos aceptados sin contar con la aprobación requerida.
- Errores en el cronograma de pagos.
- Abono de crédito errado o no abono.

4.3. IDENTIFICAR LAS AMENAZAS O CAUSAS DE RIESGOS EN EL PROCESO

Para realizar los diagramas de Causa-Efecto, primero definimos cuales serán las categorías de causas que se utilizarán. Para este caso utilizaremos las siguientes categorías:

- Procesos
- Personas
- Tecnologías
- Externo

A. DIAGRAMA DE CAUSA -EFECTO

A continuación tenemos los diagramas para los riesgos detectados:

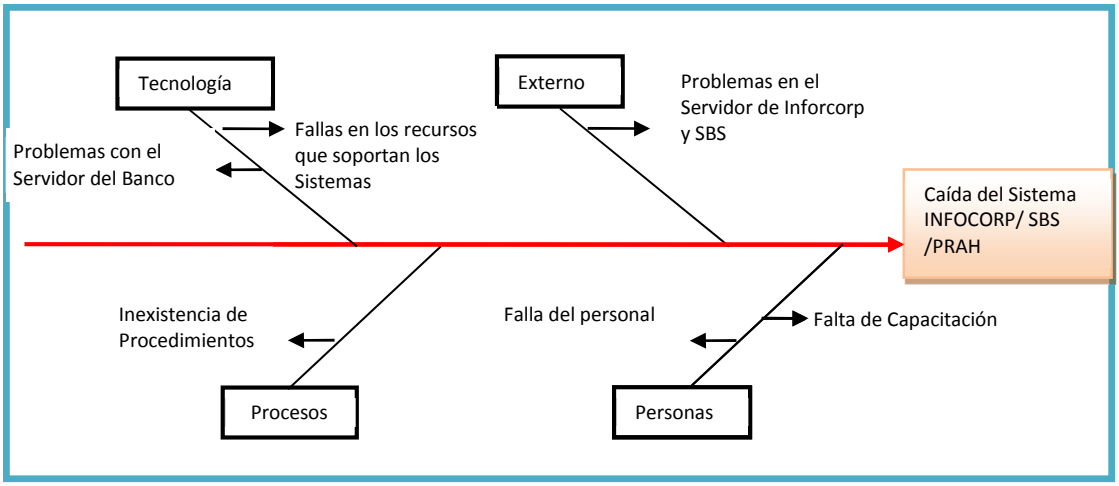


Figura 4.3 Riesgo: Caída del sistema Infocorp / SBS/ PRAH

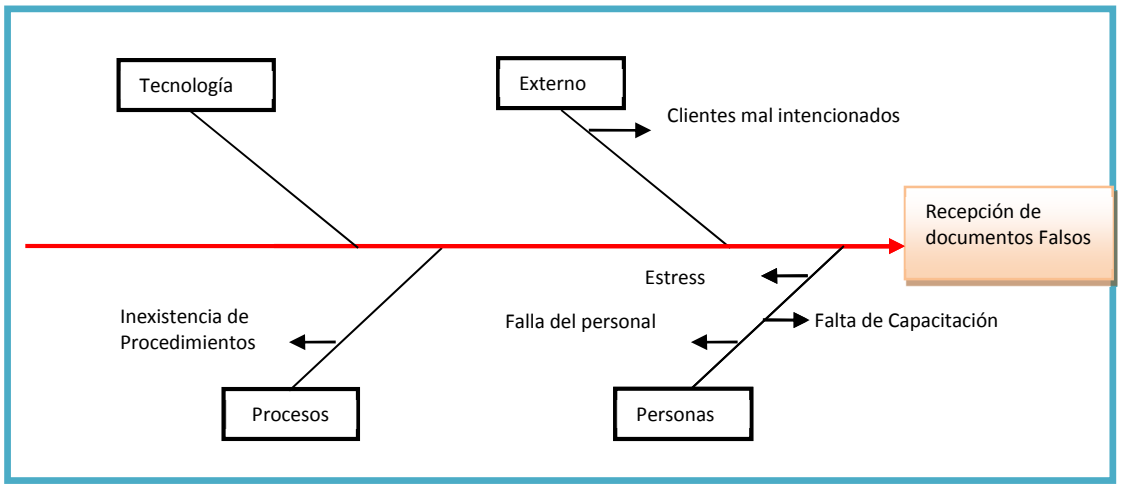
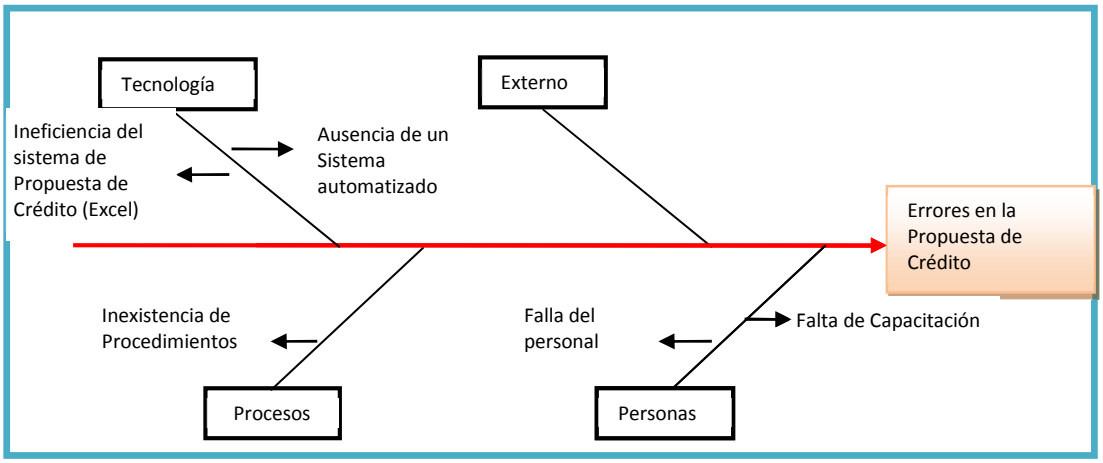


Figura 4.4: Riesgo : Recepción de documentos falsos

Figura 4.5: Riesgo Errores en la propuesta de crédito



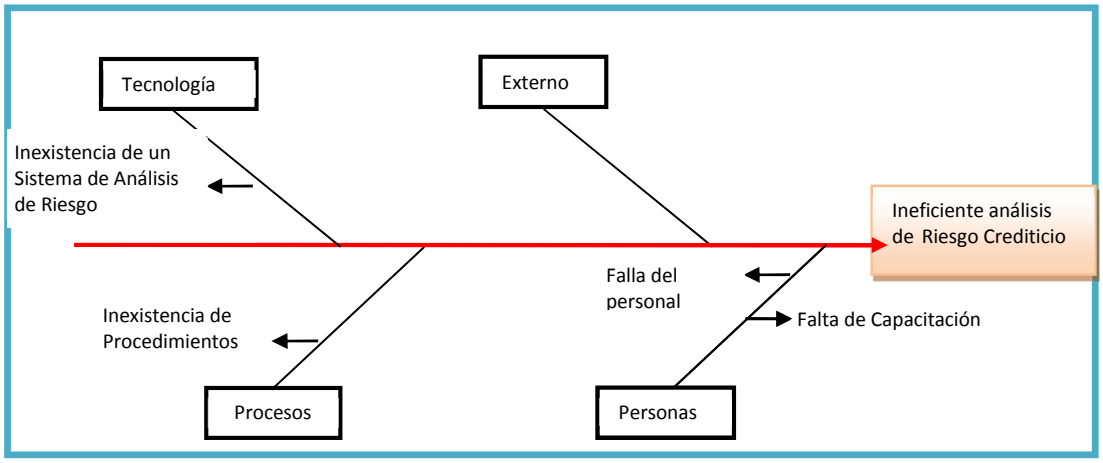


Figura 4.6: Riesgo Ineficiente análisis de riesgos crediticio

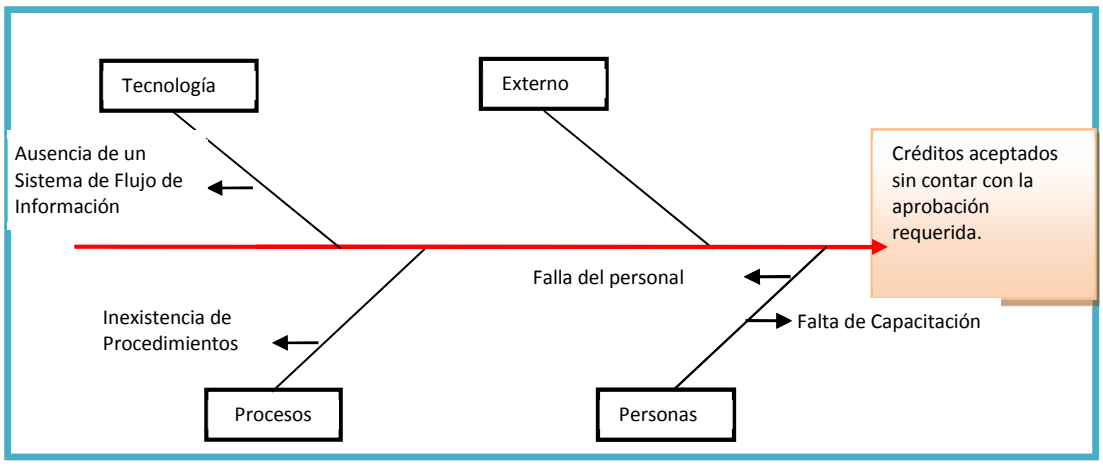


Figura 4.7: riesgo: Créditos aceptados sin contar con la aprobación necesaria

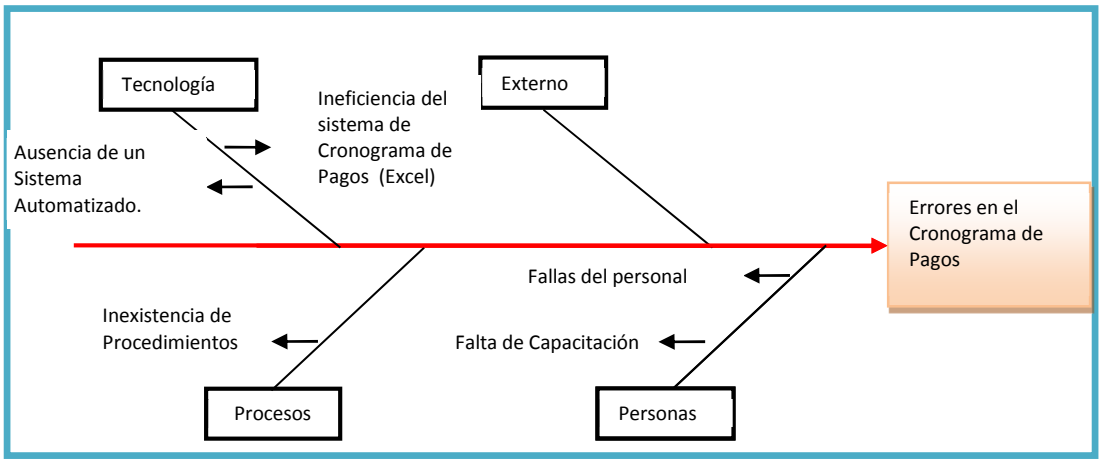


Figura 4.8: Riesgo Errores en la Elaboración del Cronograma de Pagos

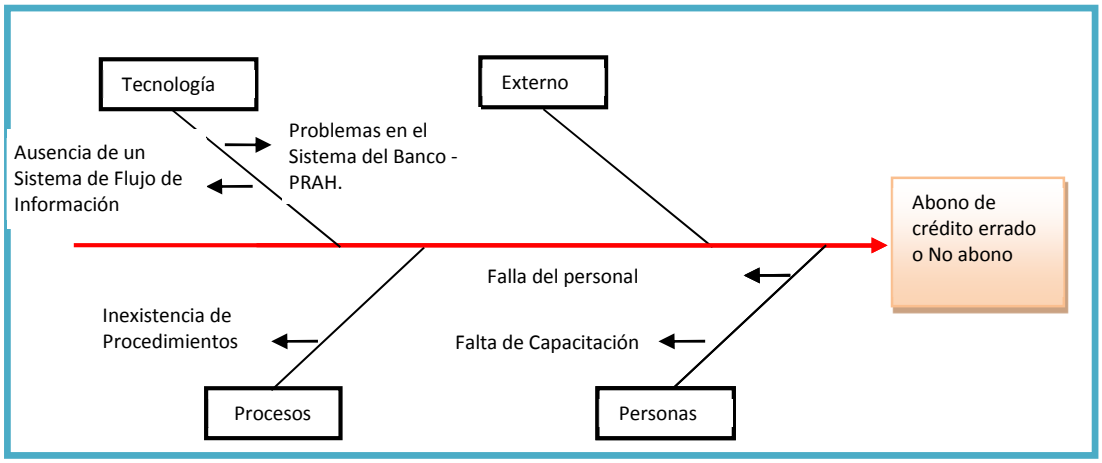


Figura 4.9: Riesgo: Abono de crédito errado o No abono

B. LISTAR LOS RIESGOS Y SUS CAUSAS DE RIESGO

Se procede a listar los Riesgos y sus causas, así como la categoría en la que se encuentran.

Estos datos se obtuvieron gracias a la técnica causa-efecto que se aplicó al Proceso Otorgamiento de Créditos a Entidades.

	EFECTO/ RIESGO	CAUSA DE RIESGO	DEFINICIÓN DE CAUSA Ó SUBCAUSA	CATEGORÍA	
	Caída del Sistema Infocorp / SBS/ PRAH	Problemas con los Servidores de Infocorp y SBS	Al ser sistemas externos, la disponibilidad depende de tales empresas.	Externo	Tecnología
		Problemas con el Servidor del Banco	Existe la posibilidad de que el Servidor se caiga causando problemas con el Sistema PRAH	Tecnología	Disponibilidad
		Falta de capacitación	El personal al no estar capacitado puede cometer errores ocasionando que algunos de los Sistemas se caiga	Personas	Recursos Humanos
		Falla del Personal	El personal, aún conociendo puede cometer errores.	Personas	Eficiencia
		Inexistencia de Procedimientos	El personal deberá tener al alcance los procedimientos para utilizar los Sistemas	Procesos	Eficiencia
R2	Recepción de documentos Falsos	Clientes/entidades presentan documentación falsa	Intención premeditada de las entidades de presentar documentación falsa para que se apruebe su solicitud de crédito.	Externo	Fraude
		Falta de Capacitación	Comete errores debido a la falta de entrenamiento	Personas	Recursos Humanos
		Falla del Personal	Existe la posibilidad de que pese a su conocimiento, el personal pueda cometer errores.	Personas	Eficiencia

		Inexistencia de Procedimientos	El personal deberá tener al alcance los procedimientos para utilizar los Sistemas	Procesos	Eficiencia
R3	Errores en la propuesta de crédito	Ausencia de un sistema automatizado para la elaboración de las pruebas.	La propuesta se efectúa de forma manual o en hojas de cálculo Excel.	Tecnologías	Infraestructura
		Ineficiencia del Sistema de Propuesta de Crédito	Al no ser un sistema automatizado puede generar errores	Tecnologías	Eficiencia
		Falta de Capacitación	El personal no conoce como realizar una propuesta de crédito o no está correctamente entrenado.	Personas	Recursos Humanos
		Inexistencia de Procedimientos.	Manual que indique los pasos para optimizar la propuesta de crédito.	Procesos	Eficiencia
		Falla del Personal	El personal puede cometer errores.	Personas	Eficiencia
R4	Ineficiente análisis de Riesgo crediticio (Dpto. Riesgos).	Falla del personal	El personal no tiene las capacidades y entrenamiento suficientes para realizar su tarea.	Personas	Eficiencia
		Inexistencia de un manual de procedimientos	Falta de un manual que indique como realizar el análisis de los riesgos crediticios.	Procesos	Eficiencia
		Falta de capacitación	El personal no ha recibido capacitación	Personas	Recursos Humanos
		Inexistencia de un Sistema Automatizado de Análisis de Riesgo	No se maneja nungún tipo de sistema.	Tecnología	Infraestructura
R5	Créditos aceptados	Falta de Capacitación	Personal no ha recibido	Personas	Recursos Humanos

	sin contar con la aprobación requerida.		capacitación necesaria.		
		Falla del personal	El personal puede cometer errores.	Personas	Eficiencia
		Inexistencia de un manual de Procedimientos	Manual de procedimientos que indiquen las tareas detalladamente.	Procesos	Eficiencia
		Ausencia de un Sistema de Flujo de Información que mantenga la información actualizada para todas las áreas.	Al realizarse de manera manual, pueden existir errores.	Tecnología	Infraestructura
R6	Errores en la elaboración del Cronograma de Pagos	Ausencia de un sistema automatizado	Los sistemas deberían ser automatizados e integrados	Tecnología	Infraestructura
		Ineficiencia del Sistema de Cronograma de Pagos	Al ser un sistema en Excel, puede traer algunos problemas, ya que no es automatizado	Tecnología	Eficiencia
		Falla del personal	Esto puede ocurrir por falta de entrenamiento	Personas	Eficiencia
		Inexistencia de un manual de Procedimientos	Manual de procedimientos que indiquen las tareas detalladamente.	Procesos	Eficiencia
		Falta de capacitación	Personal no ha recibido capacitación necesaria.	Personas	Recursos Humanos
R7	Abono de crédito errado/No abono.	Ausencia de un sistema de flujo de información.	Falta de Sistemas informáticos que integren las actividades del proceso.	Tecnología	Infraestructura
		Problemas con el Sistema de PRAH	En ese sistema se ingresa el monto y las características del préstamo, puede presentar errores o se puede caer.	Tecnología	Disponibilidad

		Falla del personal	Esto puede ocurrir por falta de entrenamiento	Personas	Eficiencia
		Inexistencia de un manual de Procedimientos	Manual de procedimientos que indiquen las tareas detalladamente .	Procesos	Eficiencia
		Falta de capacitación	Personal no ha recibido capacitación necesaria.	Personas	Recursos Humanos

Ta

Tabla 4.1 : Tabla de Riesgos y sus causas

4.4 ANALIZAR LOS RIESGOS

A. MÉTRICAS PARA LA DEFINICIÓN DE RIESGOS

Habiendo definido Los riesgos, pasamos a definir sus respectivas métricas, para medir la probabilidad o frecuencia de ocurrencia de cada riesgo, así como el impacto que ellos tienen en los objetivos del proceso.

TABLA DE PROBABILIDAD/FRECUENCIA DE RIESGOS

VALOR	PROBABILIDAD	DEFINICIÓN DE CRITERIOS
4	Permanente	Más de 10 casos al año
3	Moderado	5 casos al año
2	Ocasional	1 caso al año
1	Improbable	1 caso entre 1 y 3 años

Tabla N°4.2: Tabla de Probabilidad de Riesgos

La consecuencia de los riesgos está en que impacten en la cartera de morosos del Banco.

TABLA DE CONSECUENCIAS/IMPACTO DE RIESGOS		
VALOR	**NIVEL**	**DEFINICIÓN DE CRITERIOS**
1	Insignificante	Casi nula posibilidad de que se apruebe el crédito a una entidad morosa.
2	Marginal	Baja posibilidad de que se apruebe el crédito a una entidad morosa.
3	Crítico	Mediana posibilidad de que se apruebe el crédito a una entidad morosa.
4	Desastroso	Alta posibilidad que se le entregue crédito a una entidad morosa.

Tabla N°4.3 : Tabla de Consecuencias/Impacto

B. MAPEANDO LOS RIESGOS

Antes de definir el mapa realicemos un resumen de las causas de riesgo con su respectivo nivel de probabilidad/frecuencia y de consecuencia/impacto.

	RIESGOS	PROBABILIDAD / FRECUENCIA	CONSECUENCIA / IMPACTO
R1	Caída del Sistema de Infocorp/SBS/PRAH	4	2
R2	Recepción de documentos falsos	3	3
R3	Errores en la propuesta de crédito	3	1
R4	Ineficiente análisis de Riesgo crediticio (Dpto. Riesgos).	2	3
R5	Créditos aceptados sin contar con la aprobación requerida	3	4
R6	Errores en la elaboración del Cronograma de Pagos	3	1
R7	Abono de crédito errado/No abono	2	4

Tabla N°4.4: Análisis de Riesgo del proceso auditable.

Tomando los resultados de la tabla anterior hallamos la siguiente matriz de Riesgos:

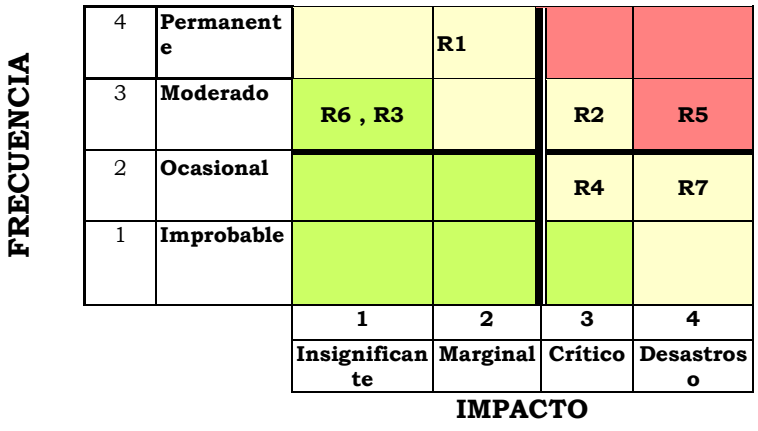


Figura N°4.10 Matriz de Riesgos

El resultado del mapa nos ofrece una guía para seleccionar los puntos de atención más importantes del Proceso auditable, tenemos que es el siguiente riesgo ubicado en la zona de color rojo:

R5: Créditos aceptados sin contar con la aprobación requerida.

Este riesgo merecen más atención, y su evaluación deberá de profundizarse, ya que son riesgos sensibles y con gran impacto para los objetivos del proceso de Otorgamiento de Créditos a entidades, por tal motivo el programa de Auditoría debe de priorizarlo.
Asimismo se deberá tomar mucha atención a los riesgos ubicados en la zona amarilla : R2,R1, R4 y R7

R2: Recepción de documentación falsa.
R1: Caída del Sistema de Infocorp/SBS/PRAH
R4: Ineficiente análisis de riesgo crediticio.
R7: Abono de crédito errado o no abono.

CAPÍTULO V

CONCLUSIONES Y TRABAJOS FUTUROS

El enfoque de auditoría a los procesos críticos de la organización y al análisis de riesgos como etapa previa para lograr mayor eficiencia en la planificación de la misma, permite orientar los esfuerzos de los generalmente limitados recursos de auditoría a procesos donde el impacto organizacional es mayor.

Una buena práctica que permite mejorar la etapa de planificación de la auditoría es realizar un adecuado análisis de riesgos, para lo cual es recomendable implementar procesos y actividades alineadas a cuerpos de conocimiento como el PMBOK, ISO y Cobit. Bajo la premisa general que los Modelos de procesos y Normas, generalmente nos dicen qué se debe implementar y no el cómo se debe hacer, es necesario que se defina qué metodología o técnica se debe utilizar para la gestión de riesgos. Una alternativa bastante aceptada como hemos visto en el contenido del presente trabajo es el de MAGERIT.

Como se ha evidenciado en el caso práctico presentado, la utilización de herramientas como el del Análisis de causa efecto, facilitan la identificación de riesgos de un determinado proceso, situación que nos facilitará al momento de realizar una auditoría de procesos, permitiendo que los auditores enfoquen su atención y programa de auditoría a aquellos riesgos críticos que afecten a la organización.

El contar con herramientas que nos ayuden a identificar y analizar los riesgos críticos de un proceso, contribuye con las necesidades de las empresas,

permitiendo que éstas puedan tratarlas y así lograr el cumplimiento de sus objetivos de operación y gestión.

Podemos mencionar a la Auditoría Continua a los Procesos como un trabajo futuro, entendemos por auditoría continua a las evaluaciones permanentes de los procesos, sin necesidad de la presencia de un auditor, porque una vez identificados los riesgos críticos se deben elaborar "alarmas" que se activarán cada vez que se pone en riesgo los objetivos del proceso.

GLOSARIO

Auditoria.

Es una evaluación y verificación sistemática, documentada, periódica y objetiva de que tan bien una entidad particular (compañía, producto, programa, individuo, destino, etc.) está cumpliendo con un conjunto de estándares.

Créditos.

La palabra **crédito** viene del latín *creditum* (sustantivación del verbo *credere*: creer), que significa "cosa confiada". Así "crédito" en su origen significa entre otras cosas, confiar o tener confianza. El crédito en general es el cambio de una riqueza presente por una futura, basado en la confianza y solvencia que se concede al deudor.

Entidad Financiera.

Banco, Caja de ahorros o cualquier otra entidad que actúe en el mercado financiero.

Informe de Auditaría.

Documento preparado por un equipo auditor en donde se expresa la opinión de un profesional frente a su evaluación.

Probabilidad.

Posibilidad de que se produzca un suceso o aparezca un valor de entre el conjunto de casos o situaciones consideradas. Clásicamente se define por el cociente de casos favorables entre los casos posibles.

Siniestro.

Es la manifestación concreta del riesgo.

REFERENCIAS BIBLIOGRÁFICAS

1. Comité de Basilea para la Supervisión Bancaria (1998), “Marco para la evaluación de los sistemas de control interno”, Basilea, Suiza.

2. Comité de Basilea de Supervisión Bancaria (2003) “Prácticas Sanas para la Administración y Supervisión del Riesgo Operativo” Basilea, Suiza.

3. Comité de Supervisión Bancaria de Basilea (2004), “Aplicación de Basi-lea II: aspectos prácticos”, Basilea, Suiza.

4. Comité de Supervisión Bancaria de Basilea (2006), “Fortaleciendo el Gobierno Corporativo en Organizaciones Bancarias”, Basilea, Suiza.

5. Rao Kolluru (1998) “Manual de Evaluación y Administración de Riesgos”, Mc. Graw Hill.

6. Rosés, Francese, (2002), “Risk Management: Una nueva forma de ase-gurar el éxito empresarial”, ACV ediciones, España.

7. Risk Management Standard 4360, (2004), Australia/New Zeland.

8. Duque A., César A, (2001), “Metodología para la gestión de riesgos”, Cé-sar Duque & Consultores de Riesgos, Colombia.

9. GUÍA PARA LAS NORMAS DE CONTROL INTERNO DEL SECTOR PÚBLICO Fr. VANSTAPEL, Primer Presidente del Tribunal de Cuentas de Bélgica, BÉLGICA, 2005

10. S. Grey, John Wiley & Sons Chichester (1995) “Practical Risk Assessment for Proyect Management”, EE.UU.

11. Henry J. Johanssen, Patrick Mc Hugh, A. John Pendlebury, William A. Wheeler III (1994), “Reingeniería de procesos de negocio”, Editorial LIMUSA S.A., México.

12. Mantilla, Samuel Alberto (2002), "De los riesgos de auditoría a los riesgos de negocio: El cambio de modelo", España.

13. Navarrete, Hernando Mariño (2001), "Gerencia de Procesos", Alfaomega Colombiana S.A., Colombia.

Tesis

14. Lorena Carmino moreno Jimenez,La auditoría en informática. Universidad de Colima, Tesis (2003). Colima – México

15. Elmer Zanabria, Enfoque de auditoría de gestión presupuestaria al Sector Público: Region Puno, Tesis Magister (2003), Lima –Perú

16. Duran Bellonch, Maria del Mar, Auditoría cultural de una empresa de alta tecnología como un procedimiento inicial en la implementación de una estrategia de formación continua, Tesis (2002), Barcelona-España

Direcciones Electrónicas

17. Jacqueline Huamankenny Vela, Alto Voltaje, Universidad de Lima, http://www.ulima.edu.pe/webulima.nsf/default/alppp?OpenDocument&dn=1.2.4, 10/03/2008

18. Análisis y Mejoramiento de Procesos, Esan, http://www.esan.edu.pe/paginas/publicaciones/, 30/04/2008

19. Procesos y Mapas Estratégicos, Microsoft, http://download.microsoft.com/documents/uk/resources/rkaplan.pdf, 15/04/2008

20. Aldo Bresani, Mejoramiento de las fases de los procesos, ESAN, http://www.esan.edu.pe/paginas/publicaciones/, 20/03/2008